

Fig. 1A
(Prior Art)

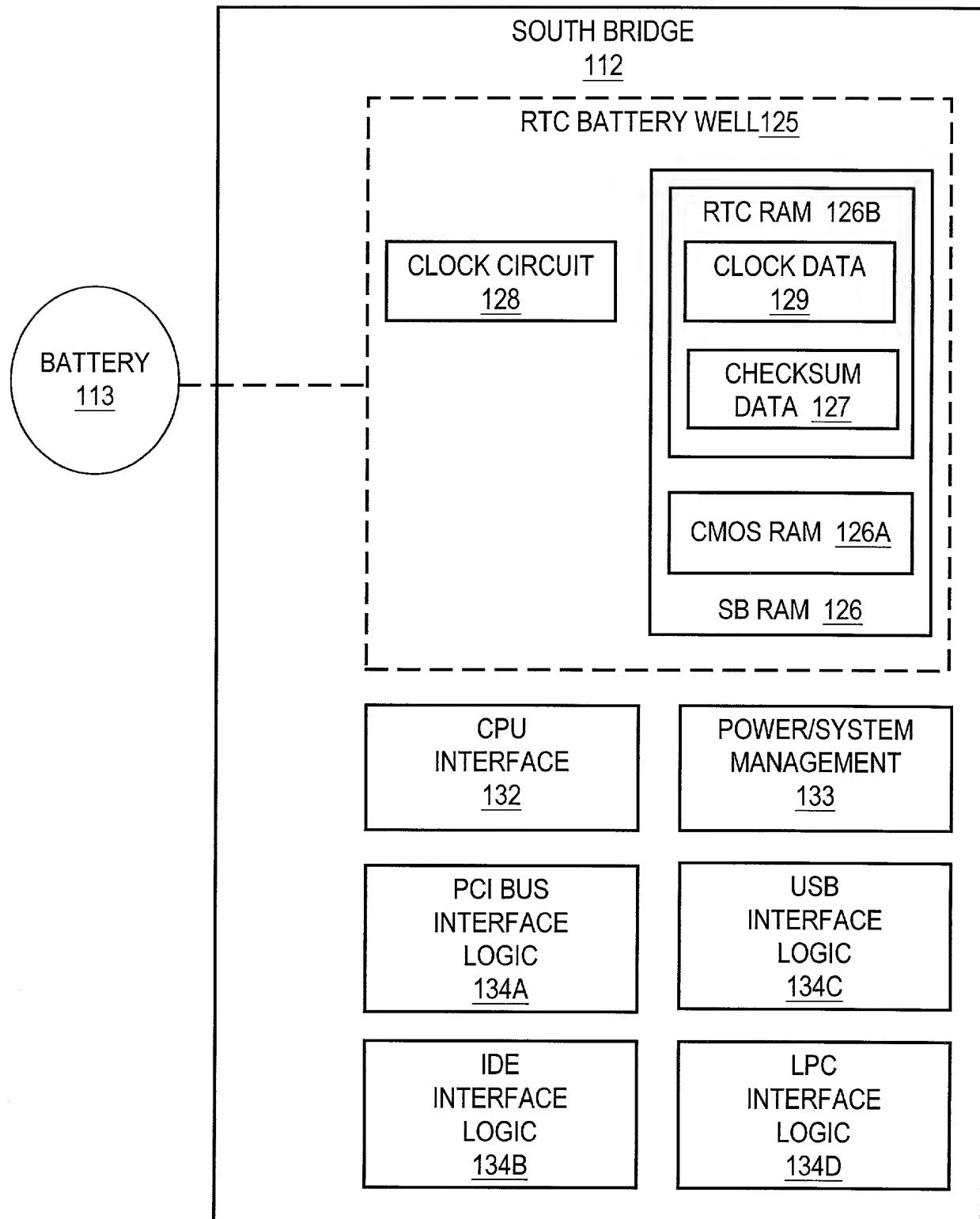


Fig. 1B
(Prior Art)

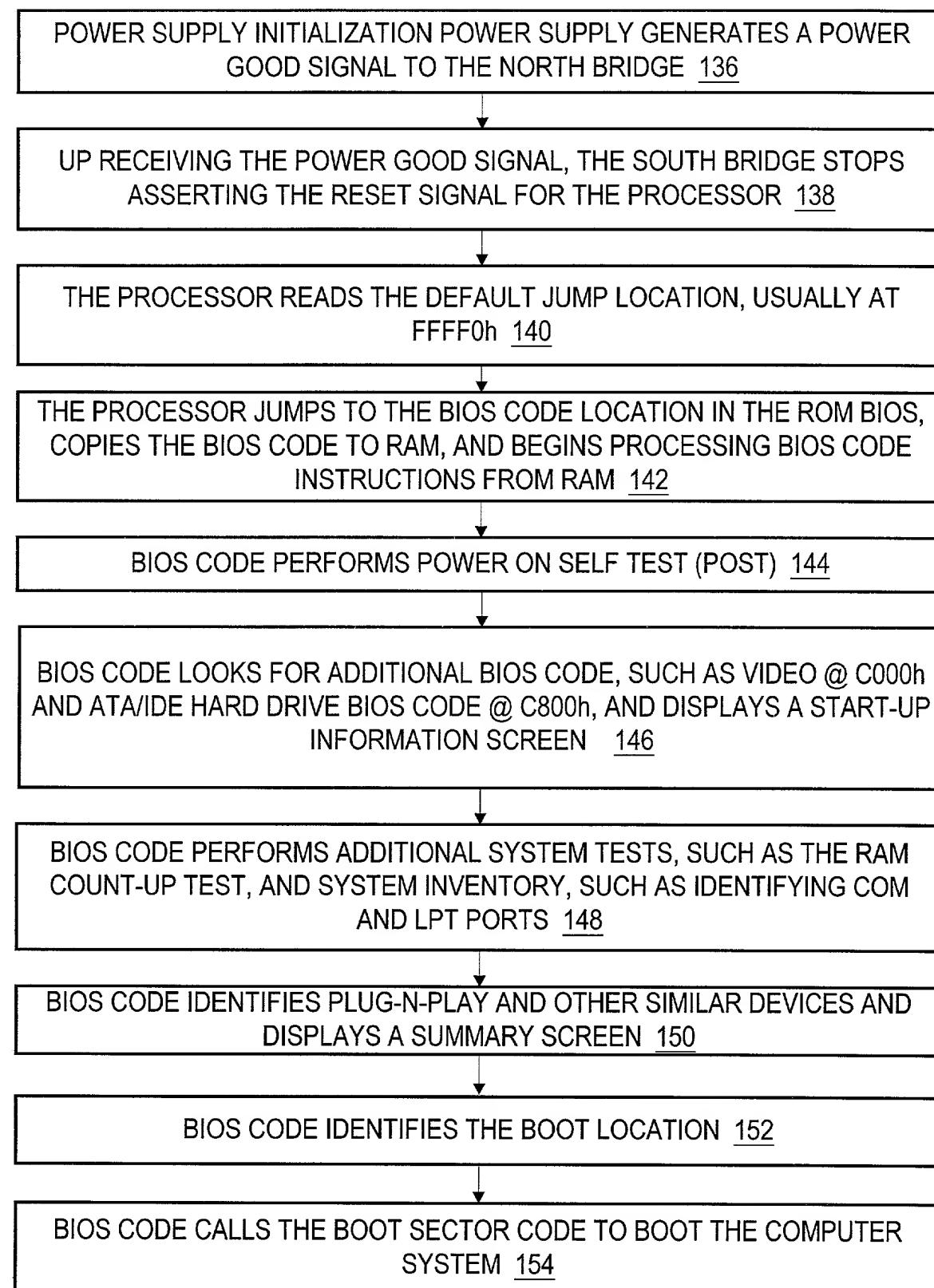


Fig. 2A
(Prior Art)

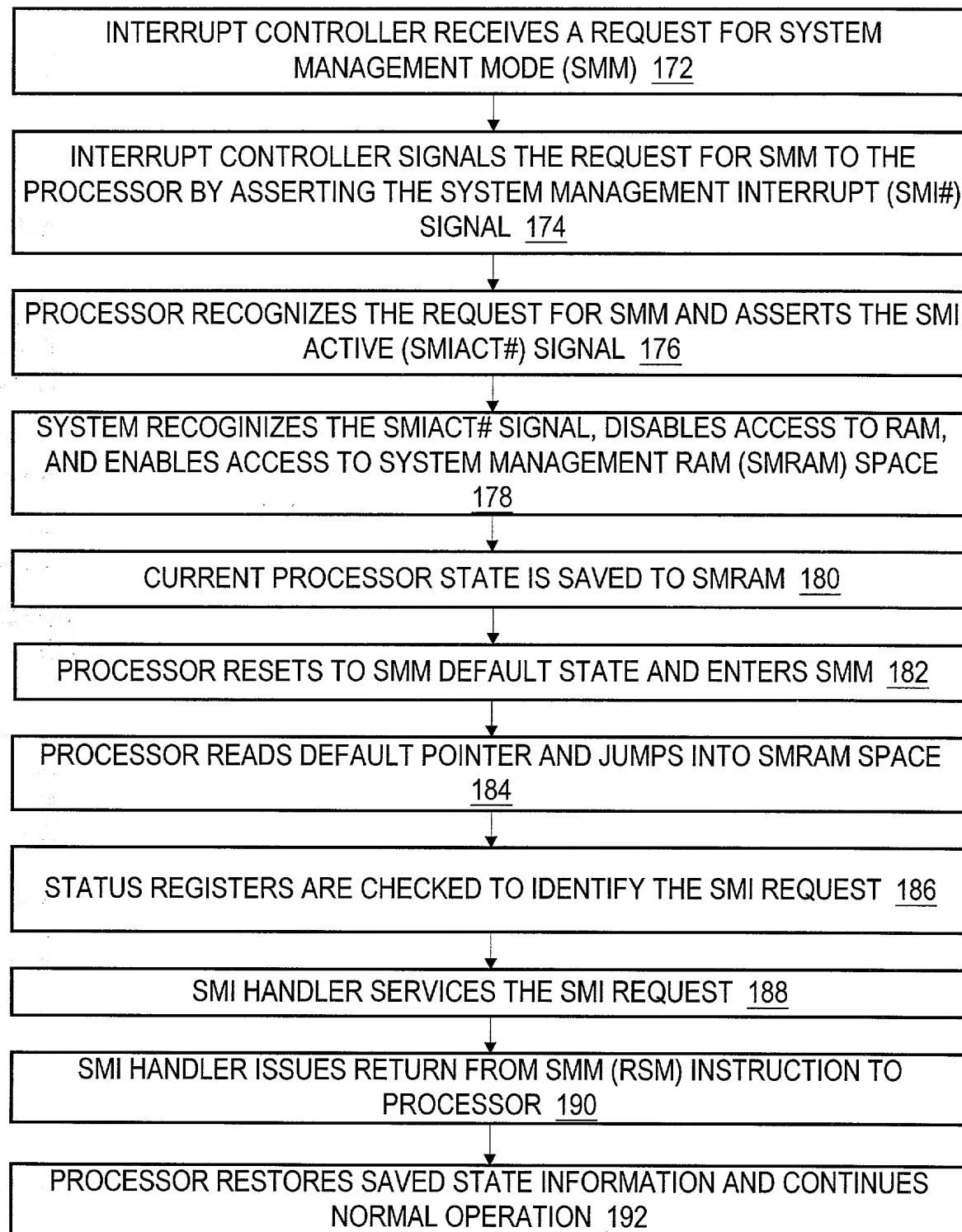
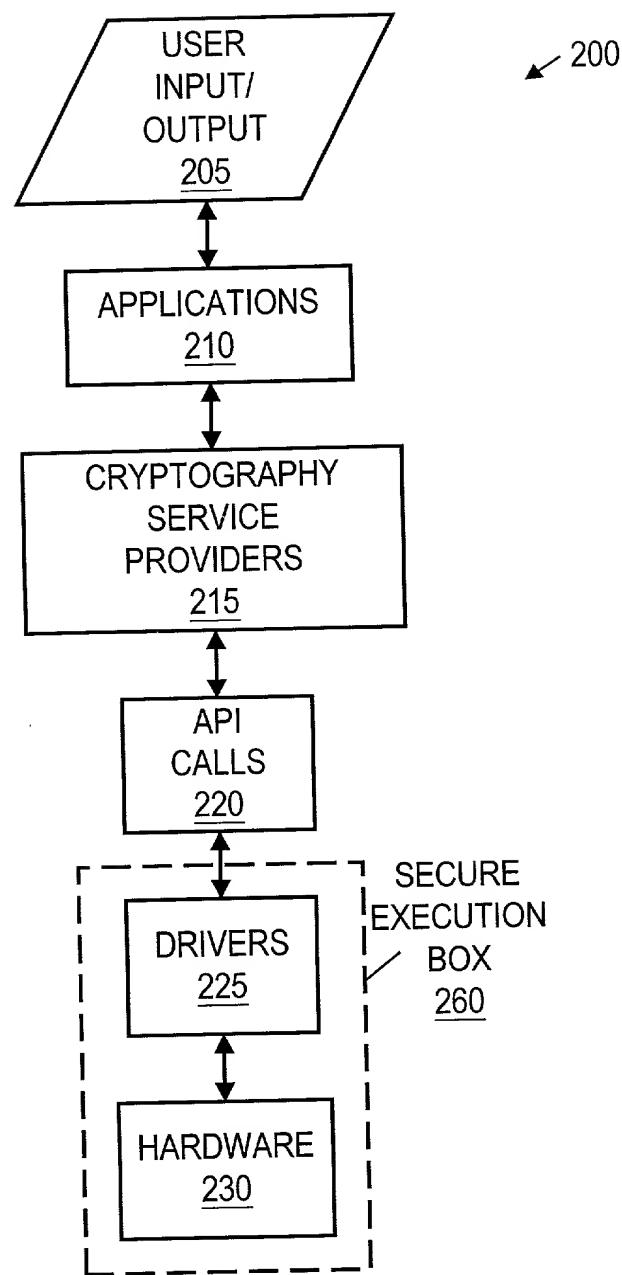
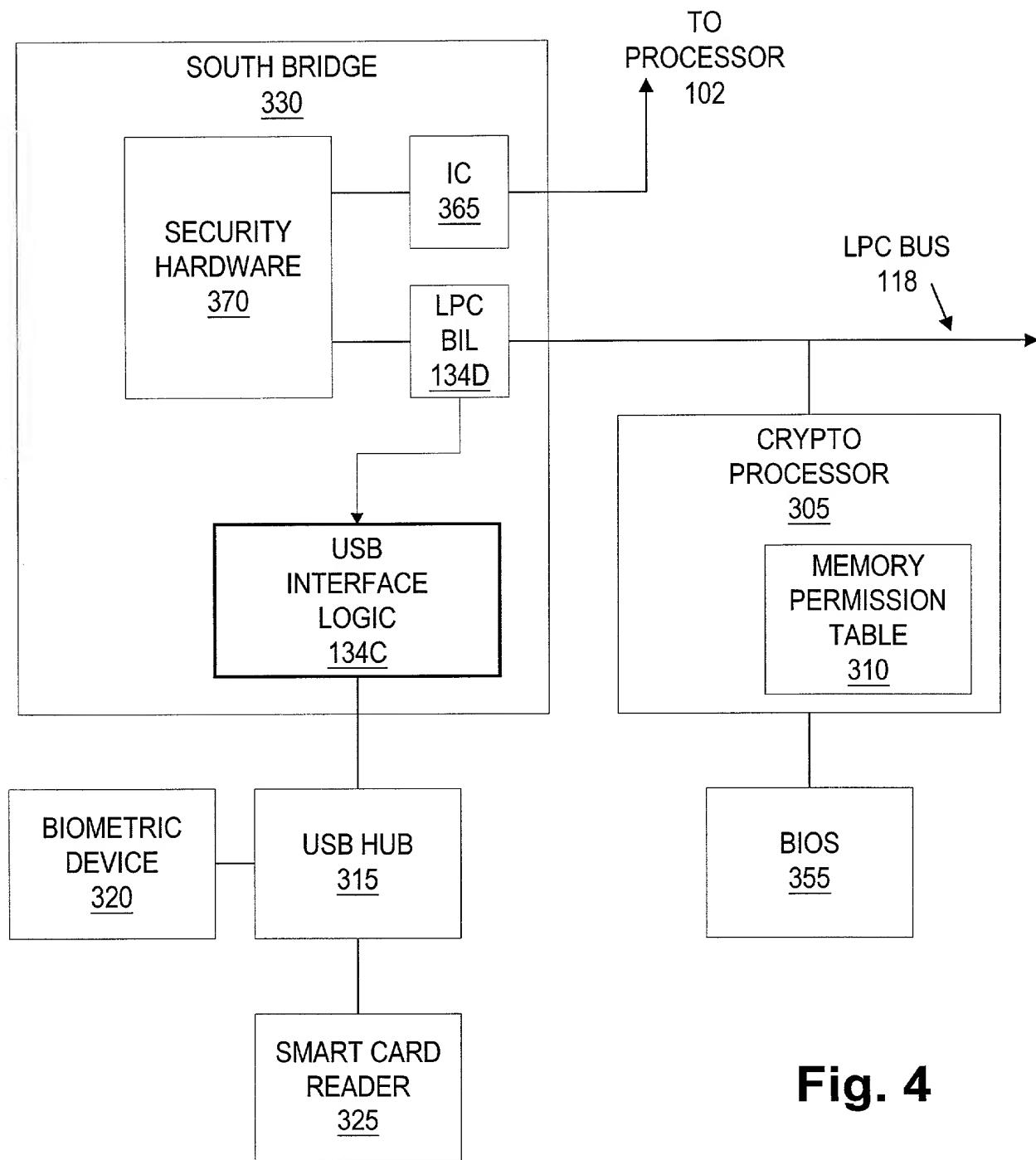
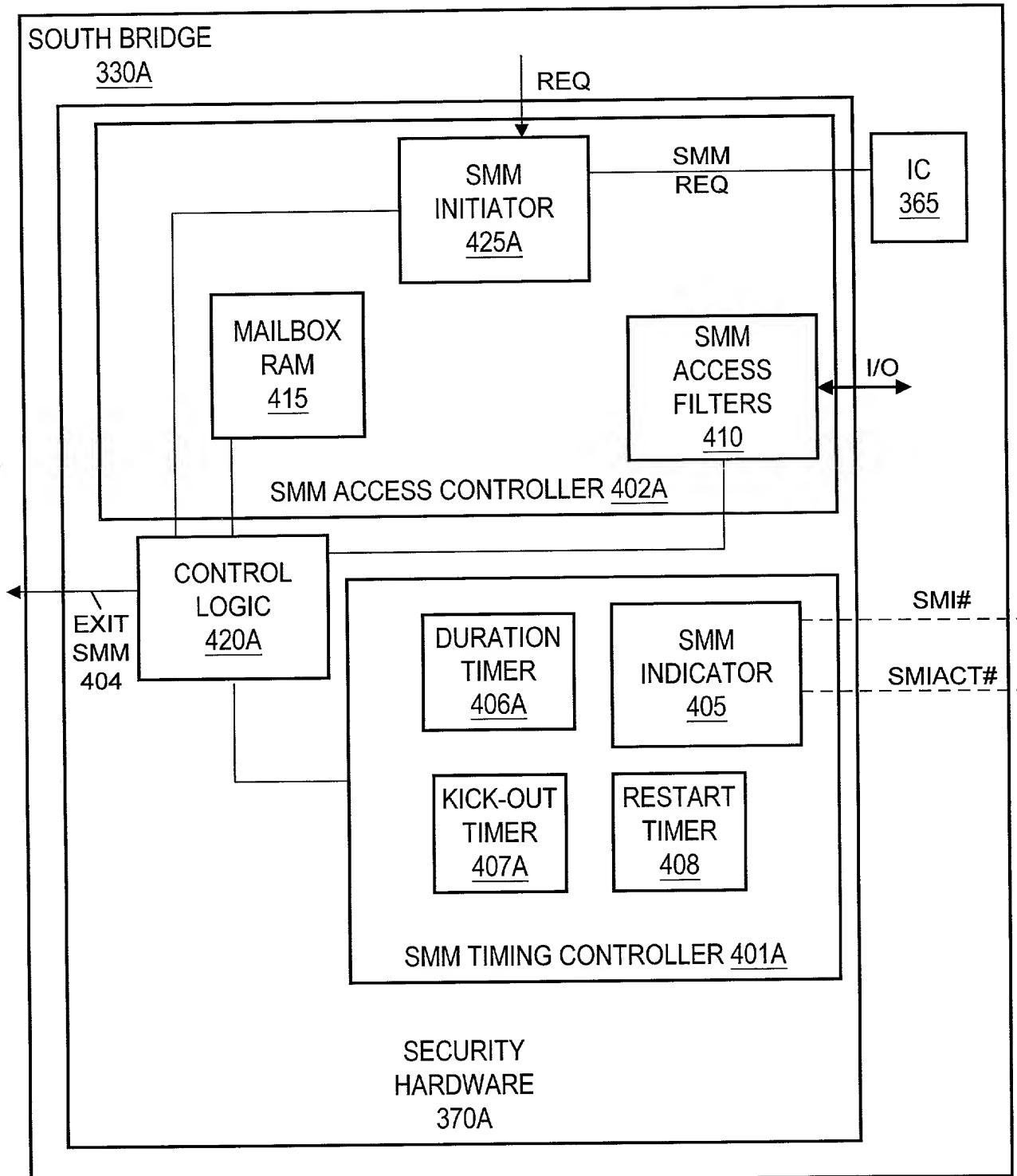
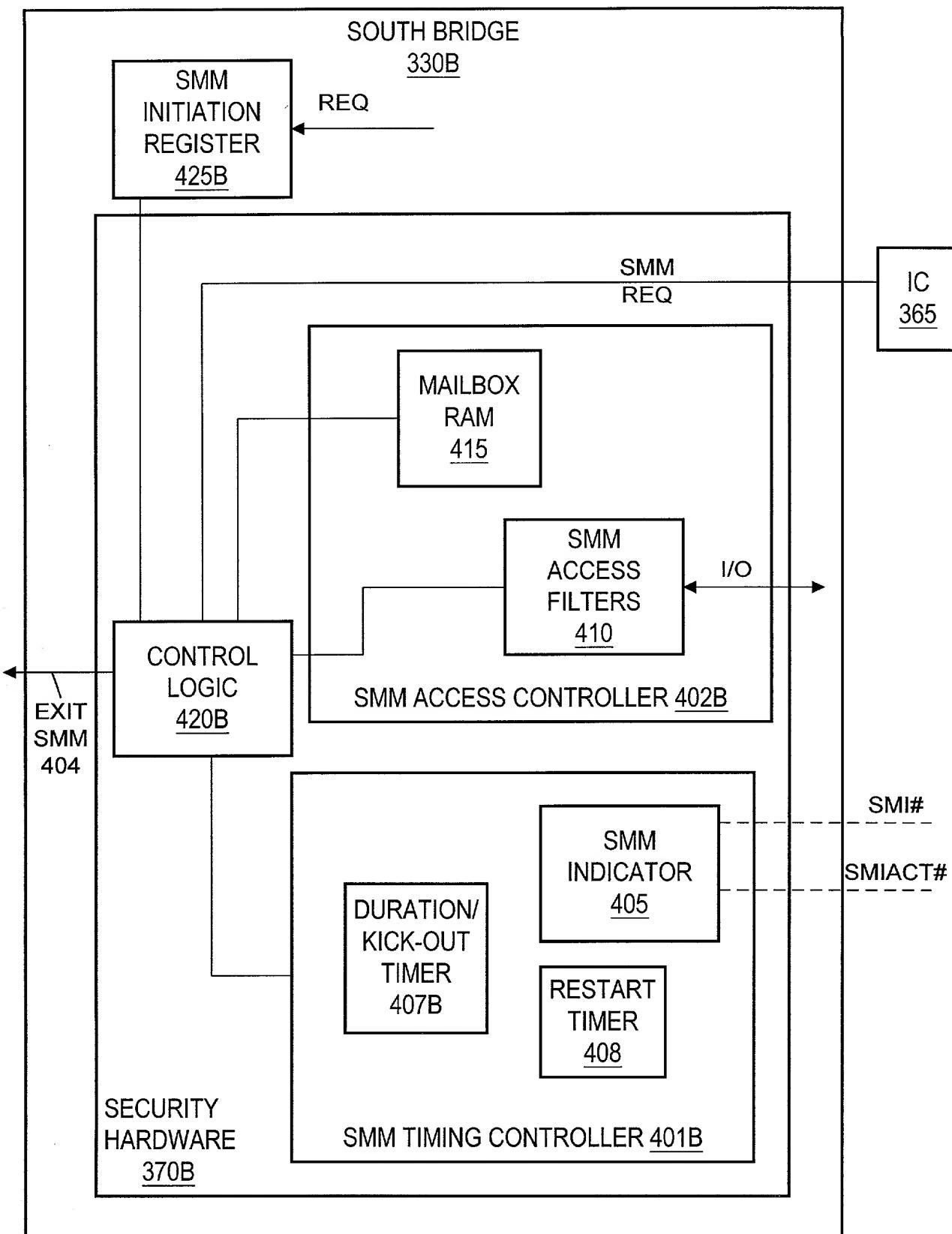


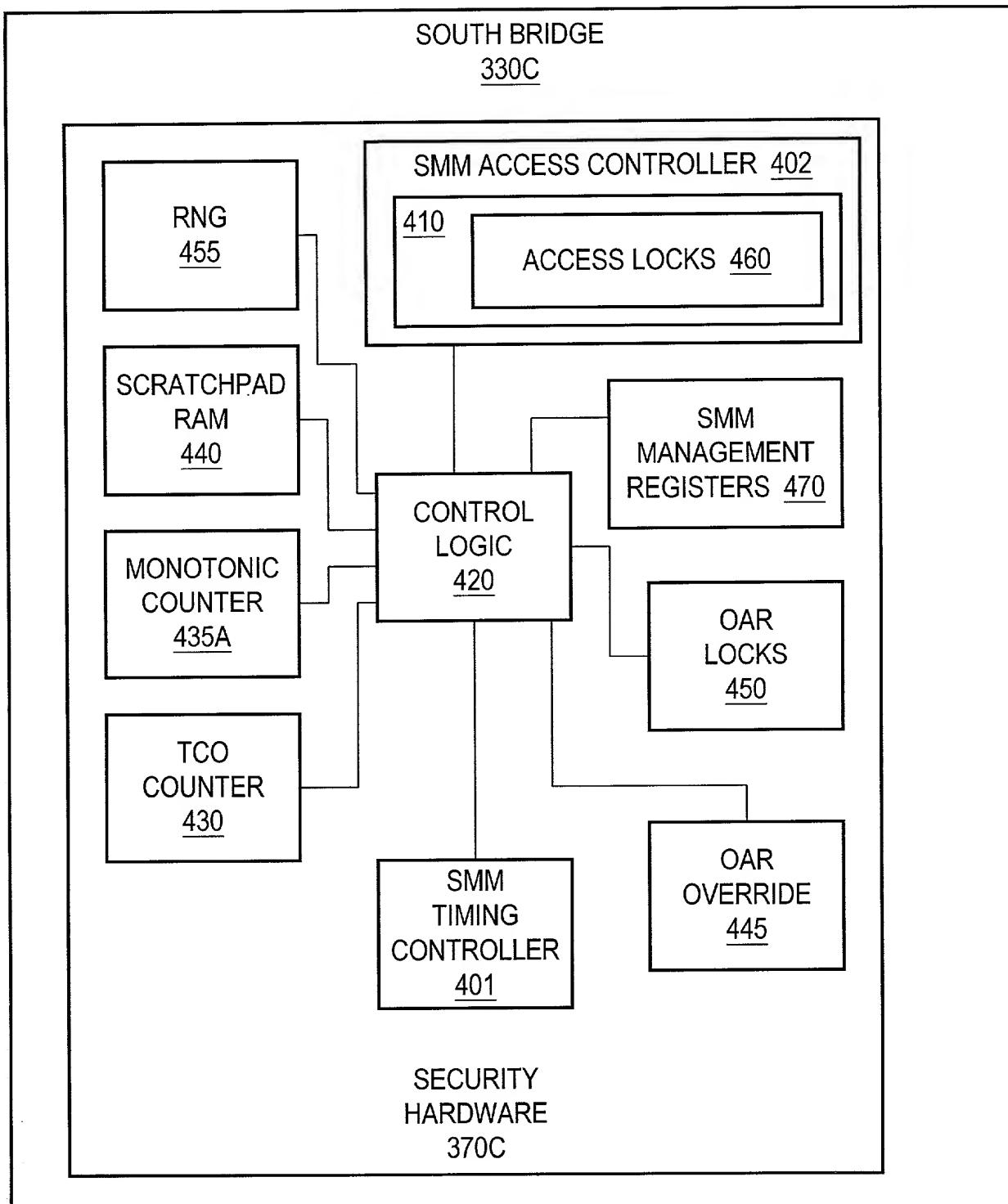
Fig. 2B
(Prior Art)

**Fig. 3**



**Fig. 5A**

**Fig. 5B**

**Fig. 6**

10 / 73

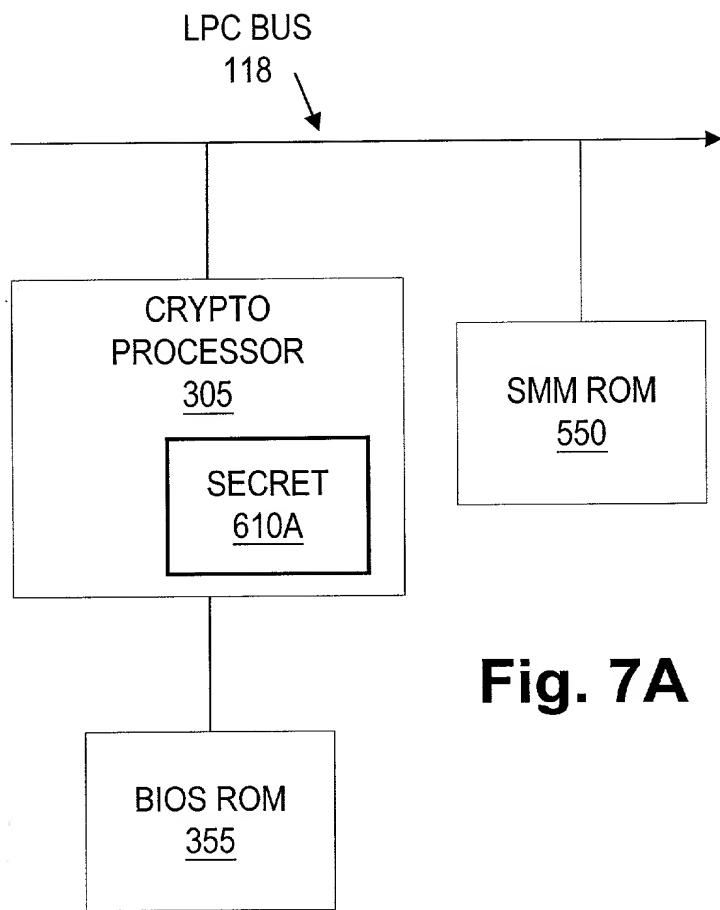


Fig. 7A

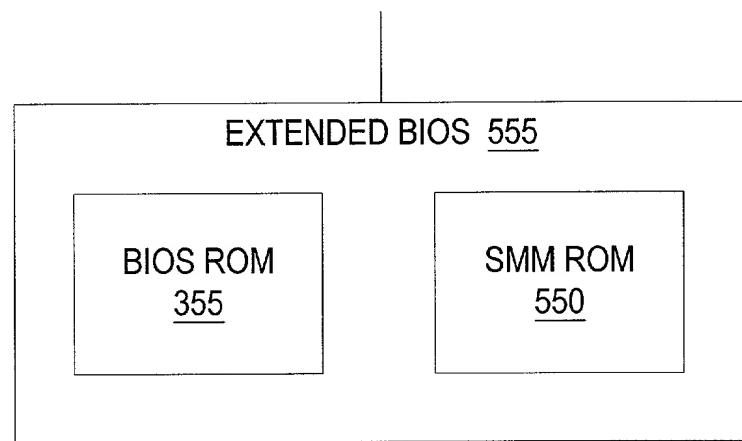


Fig. 7B

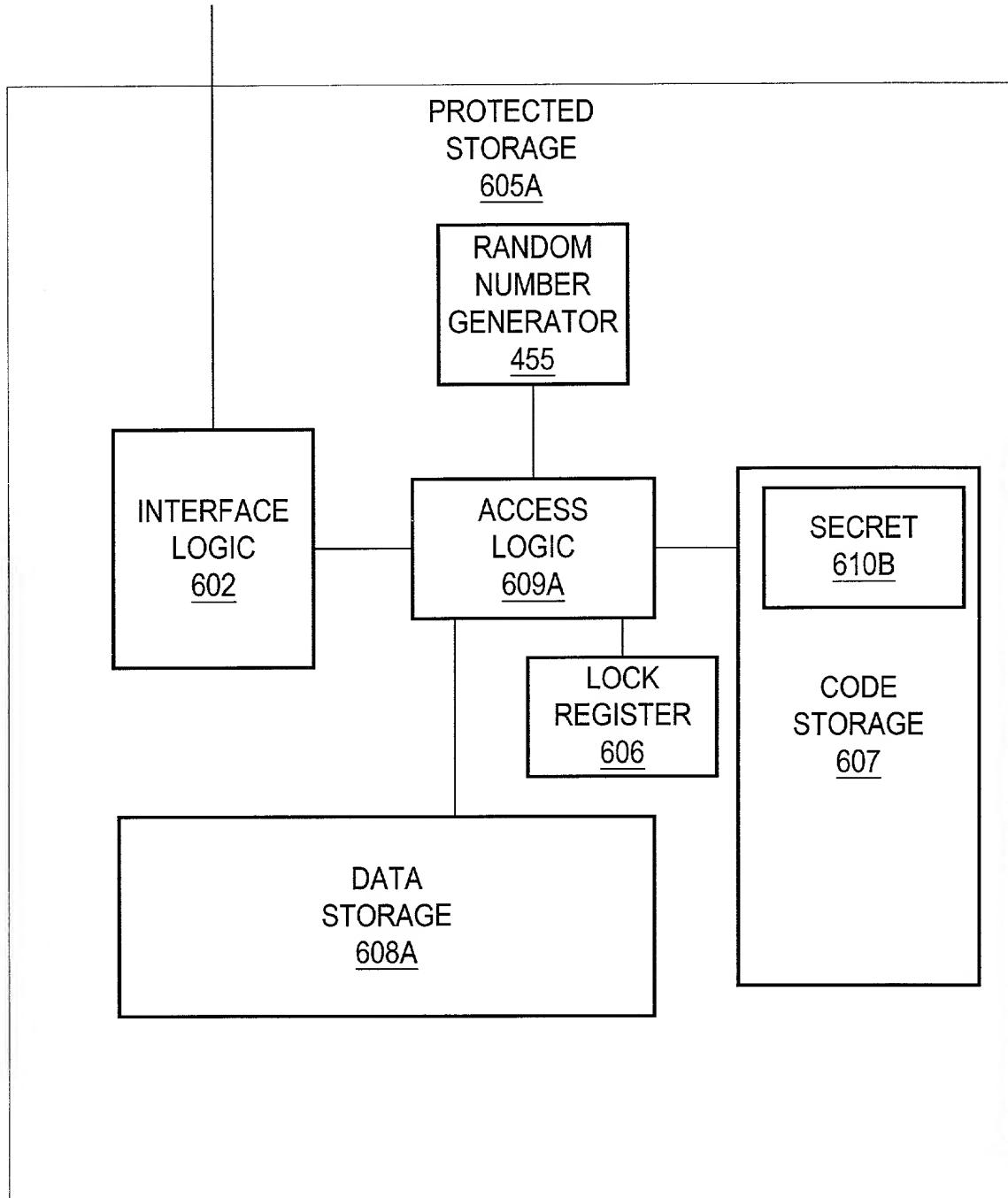


Fig. 7C

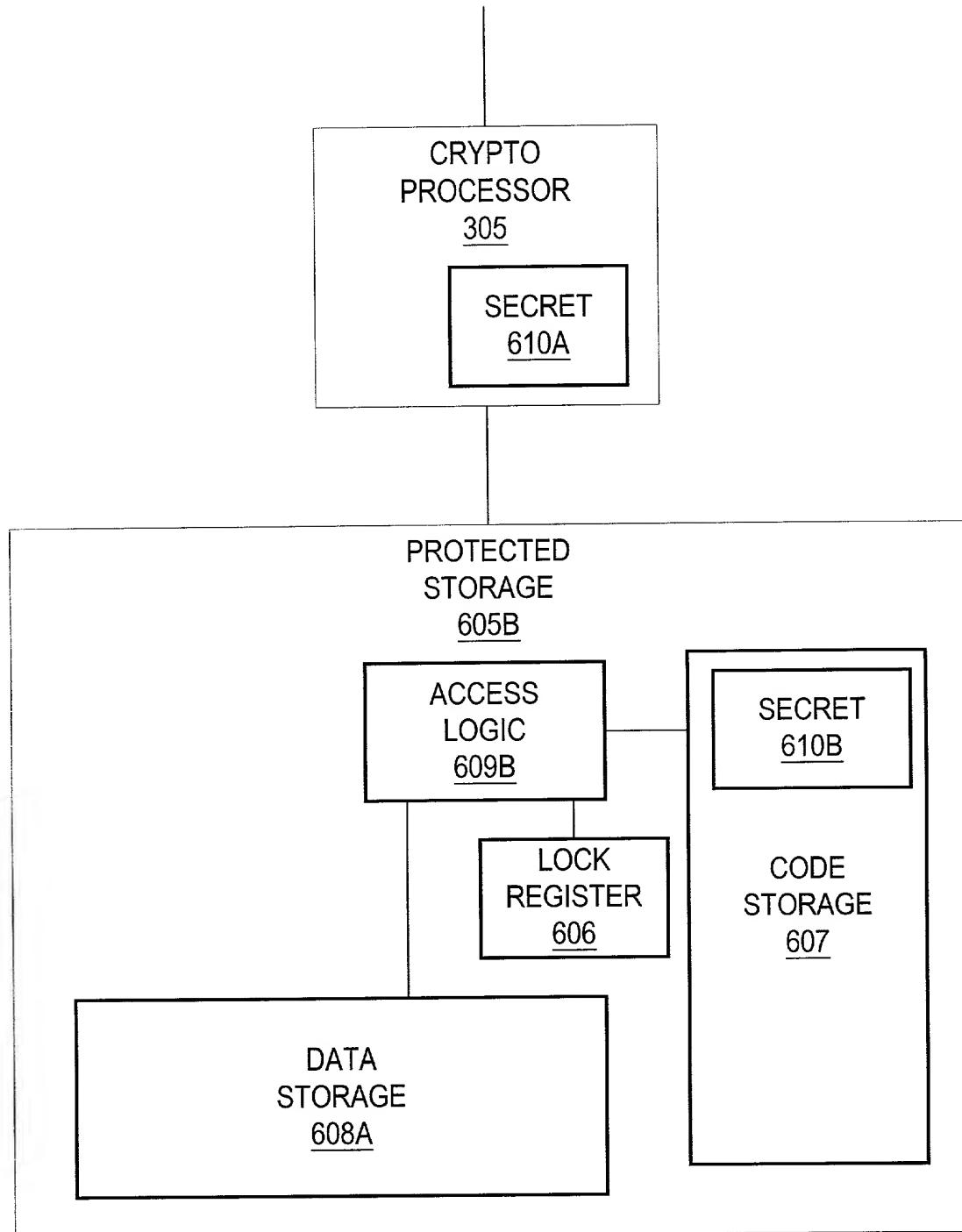


Fig. 7D

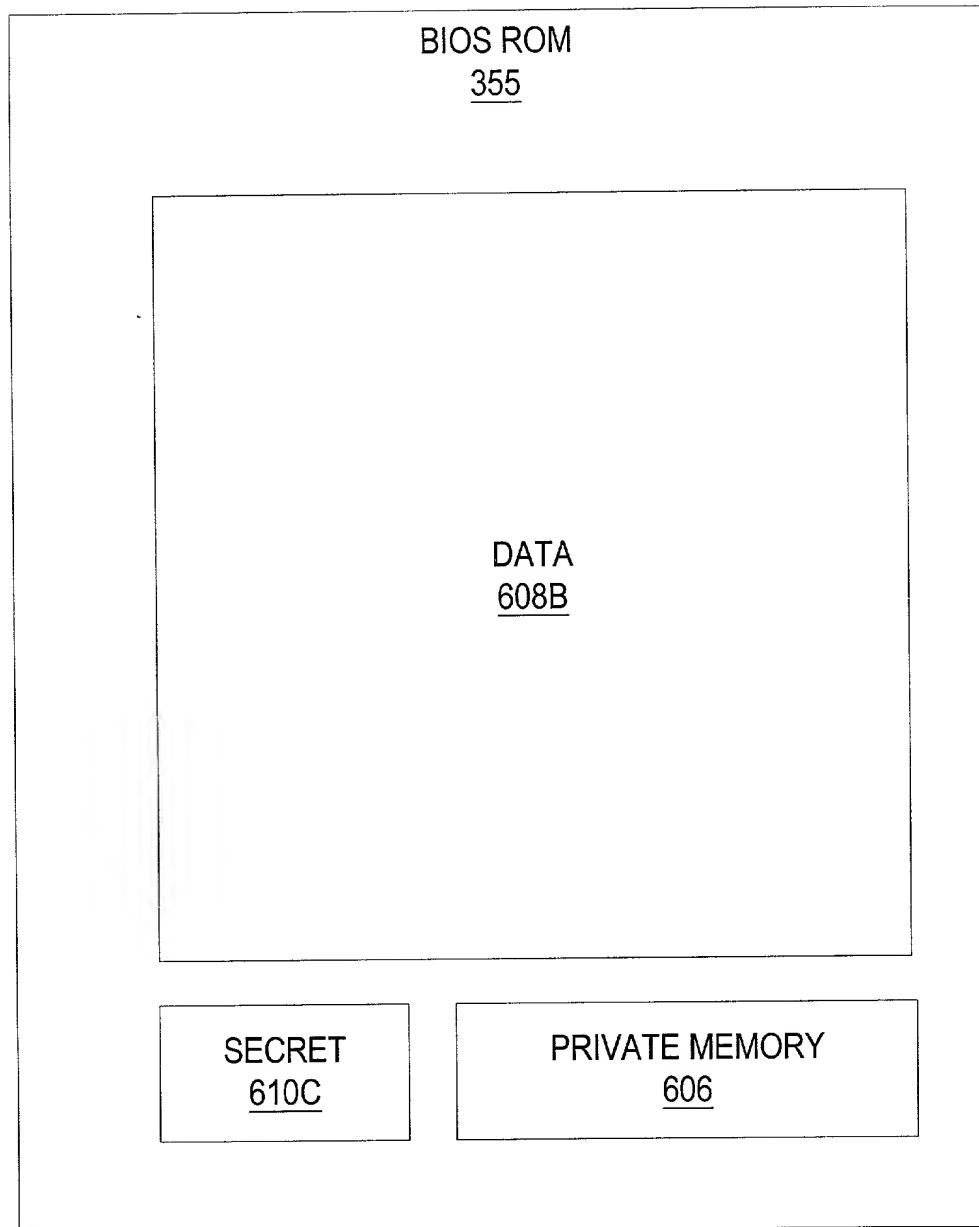


Fig. 8A

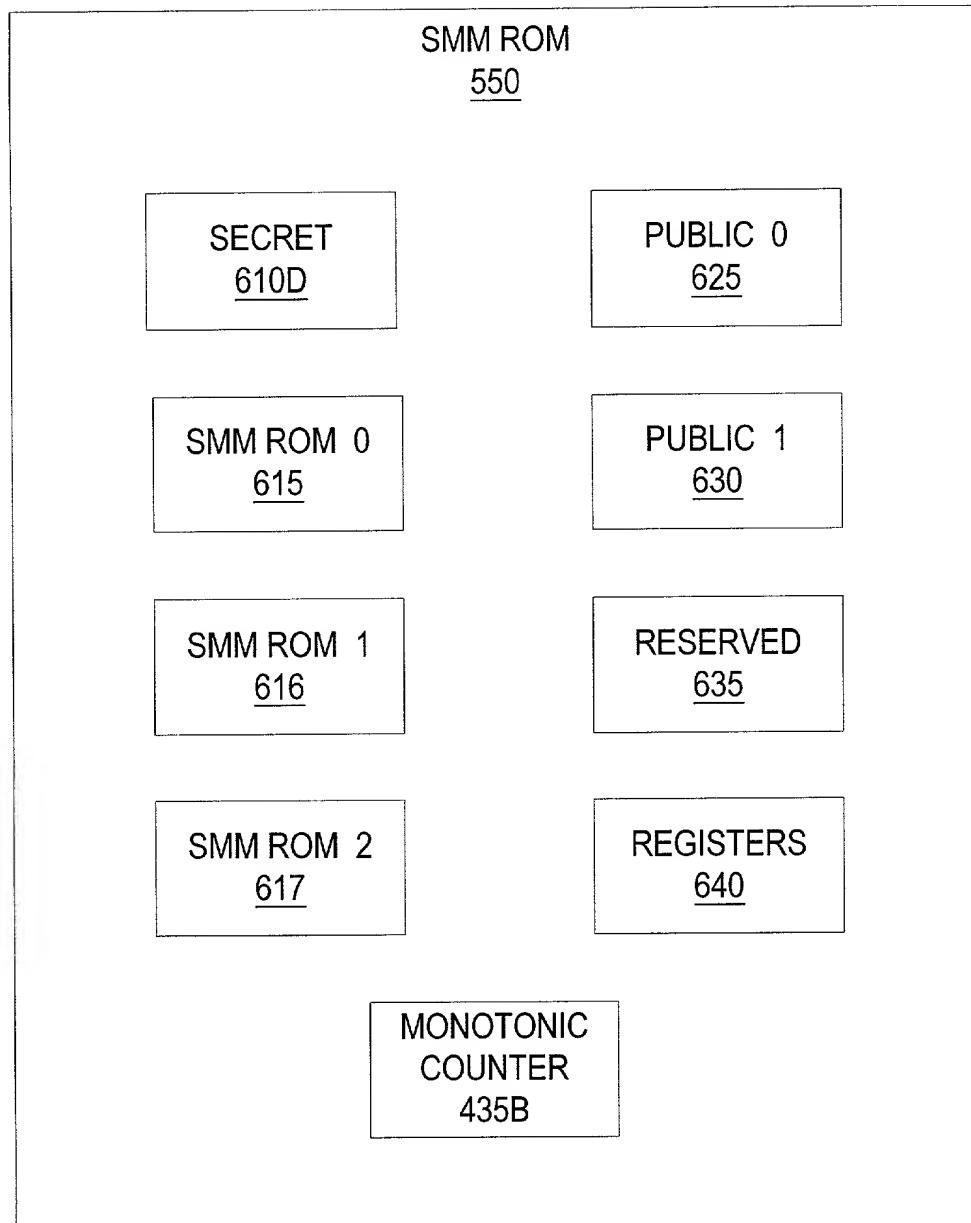


Fig. 8B

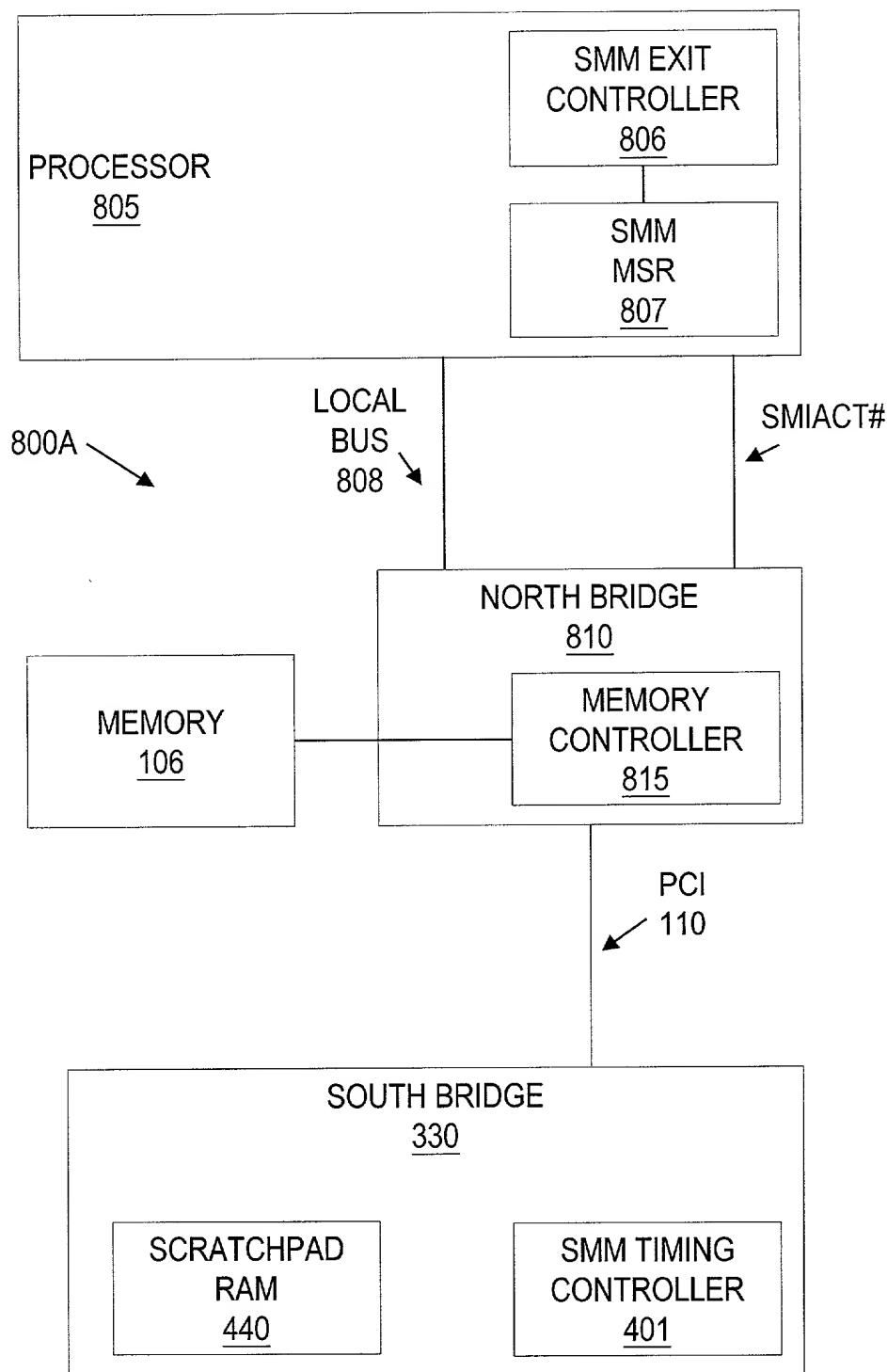


Fig. 9A

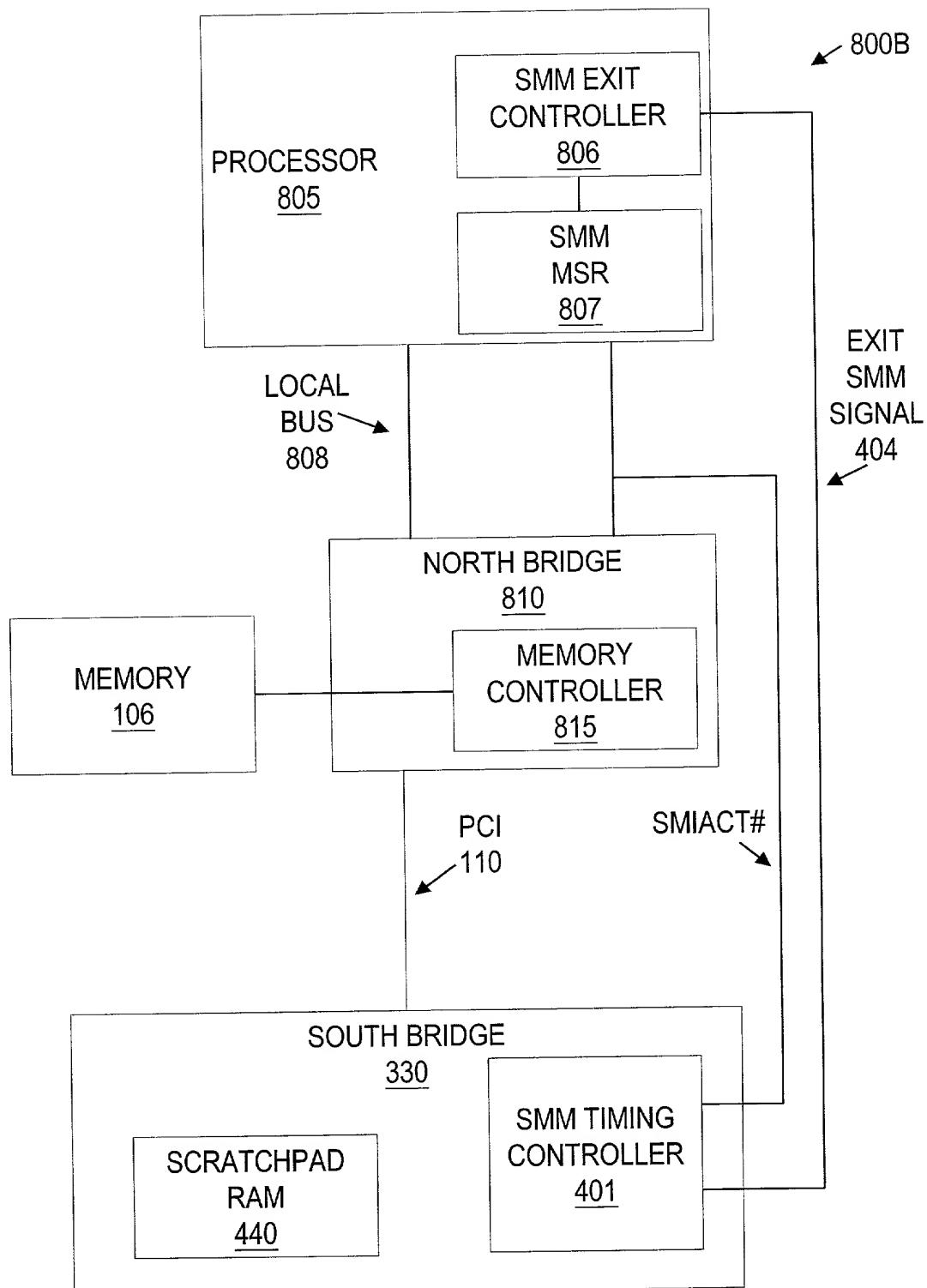


Fig. 9B

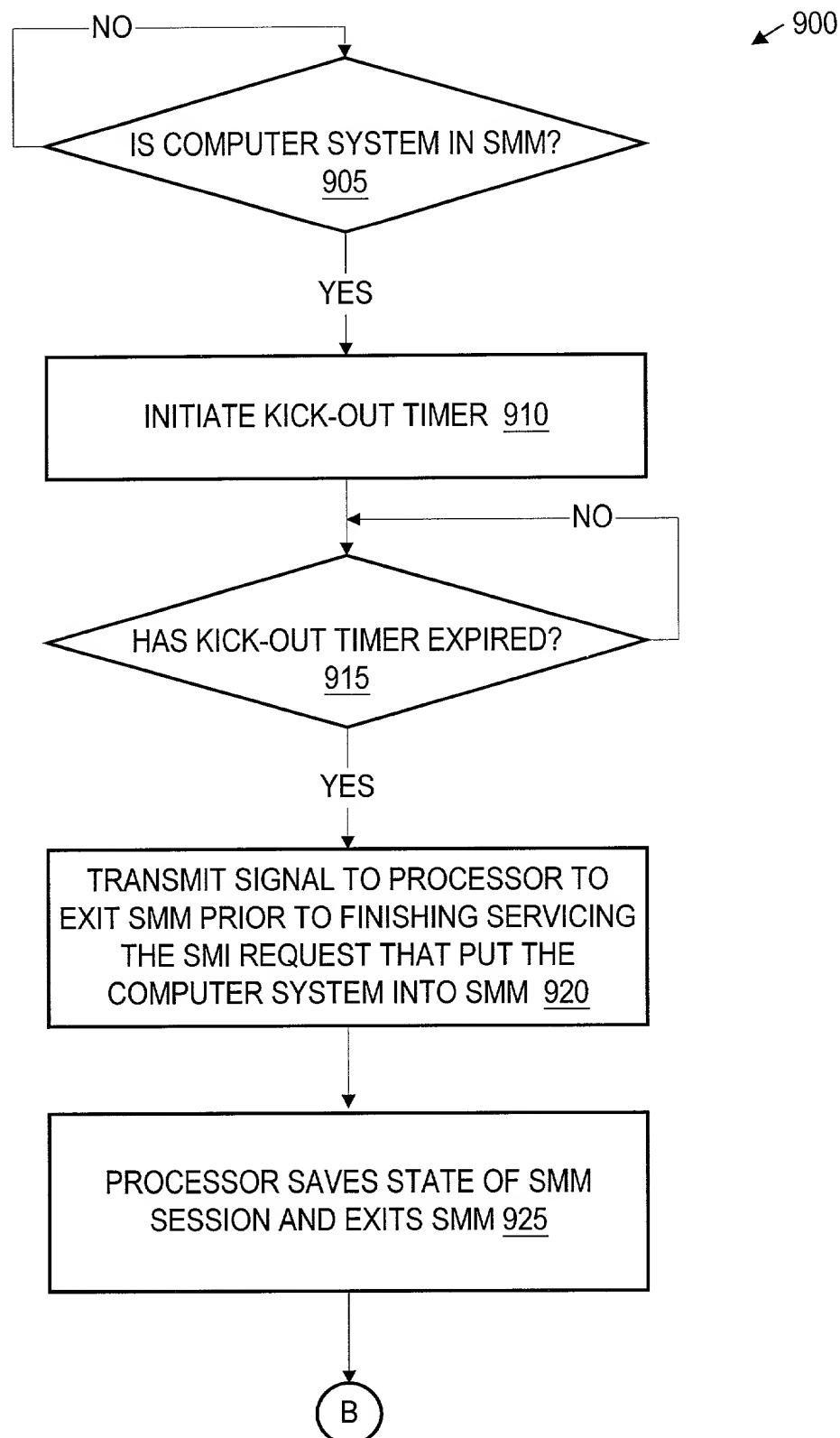


Fig. 10A

18 / 73

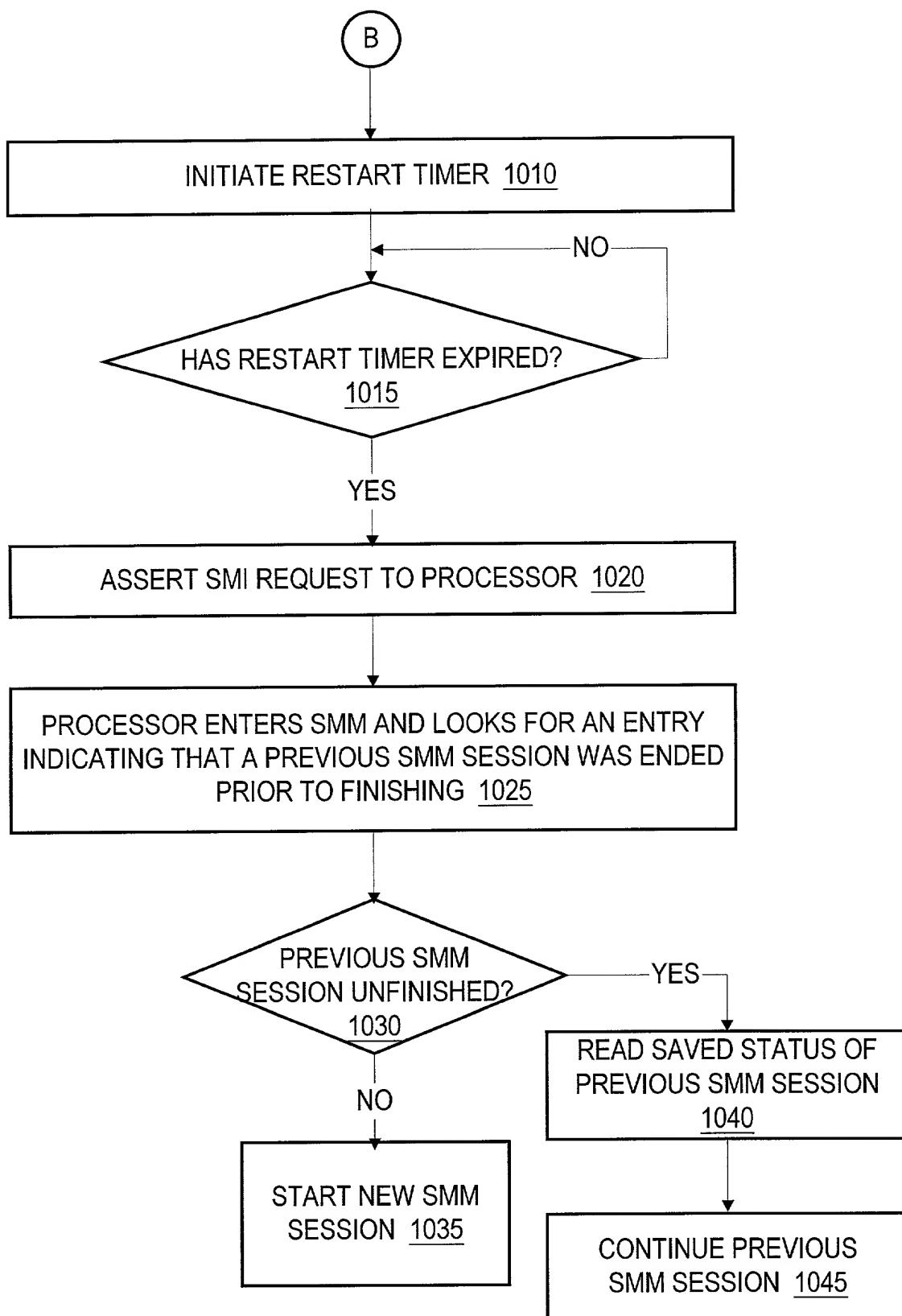


Fig. 10B

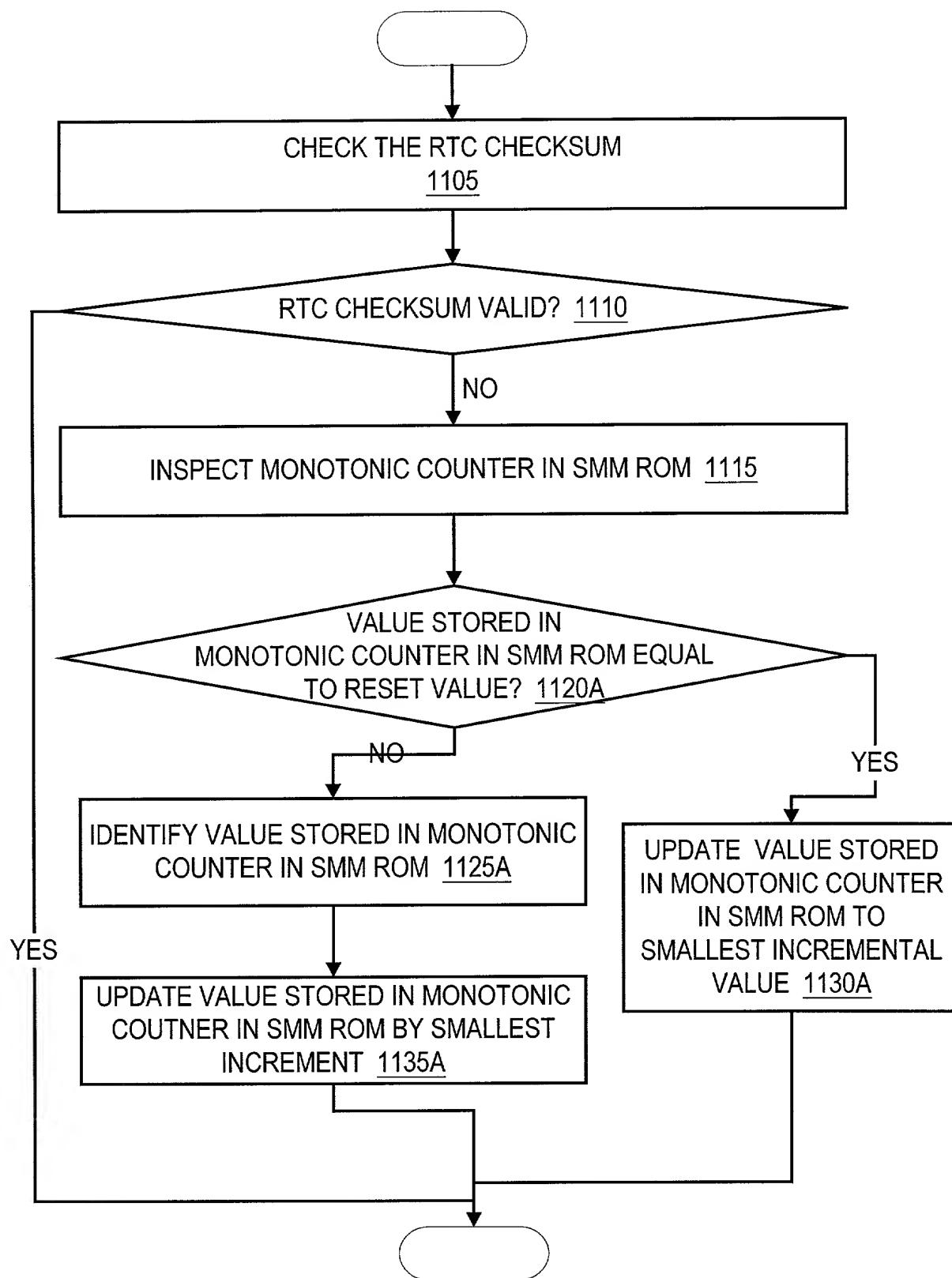


Fig. 11A

20 / 73

1100B

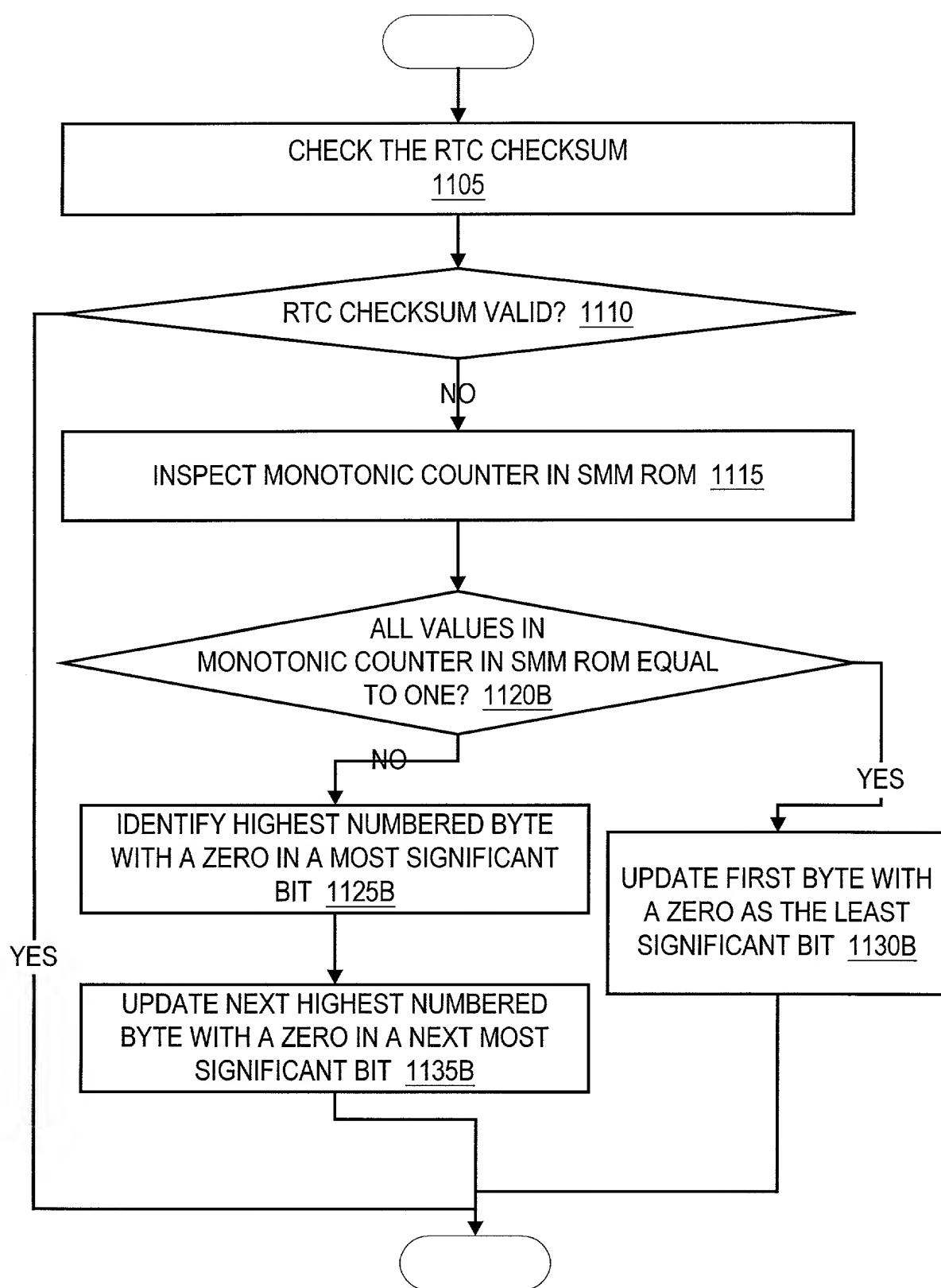


Fig. 11B

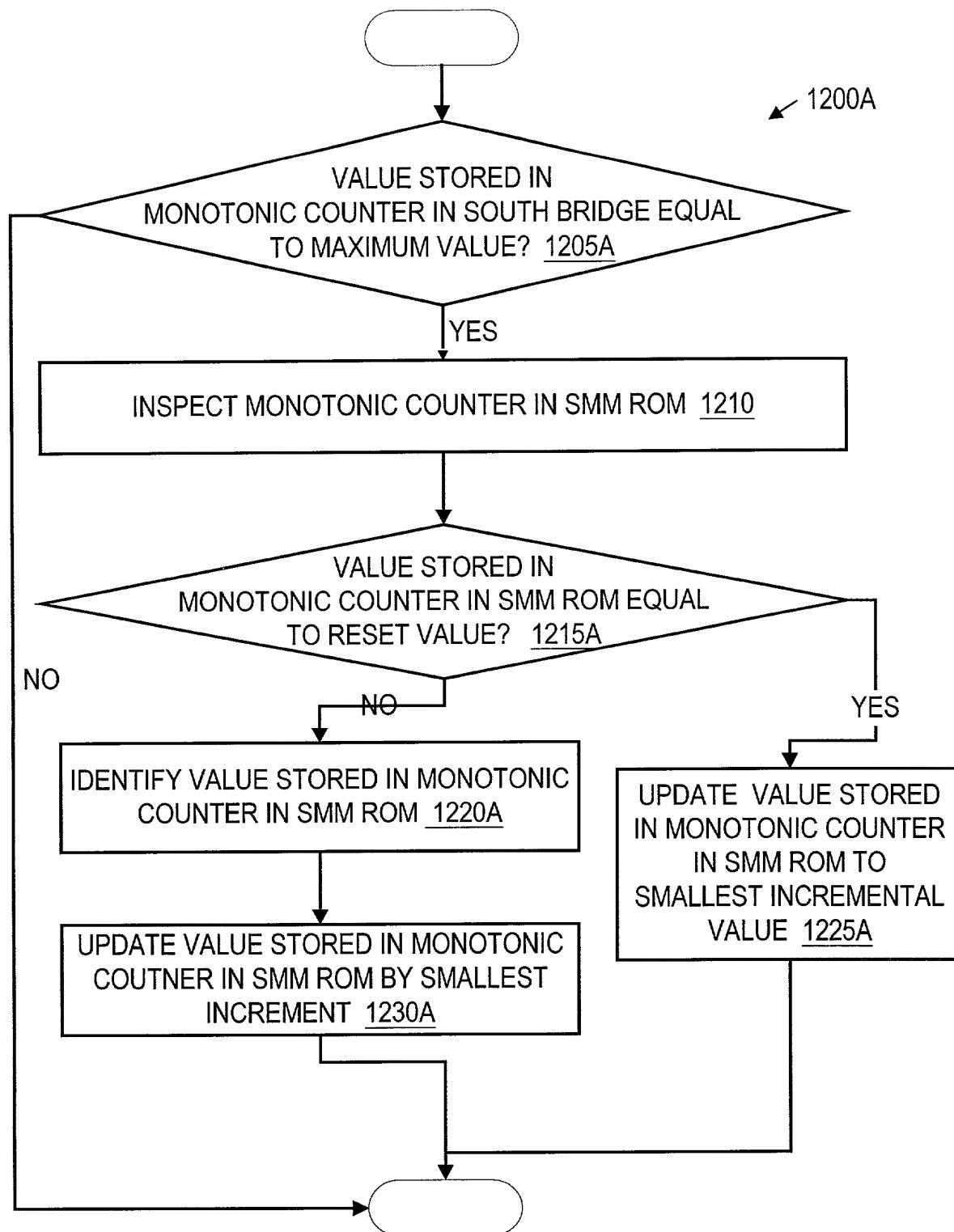


Fig. 12A

03853226 054104

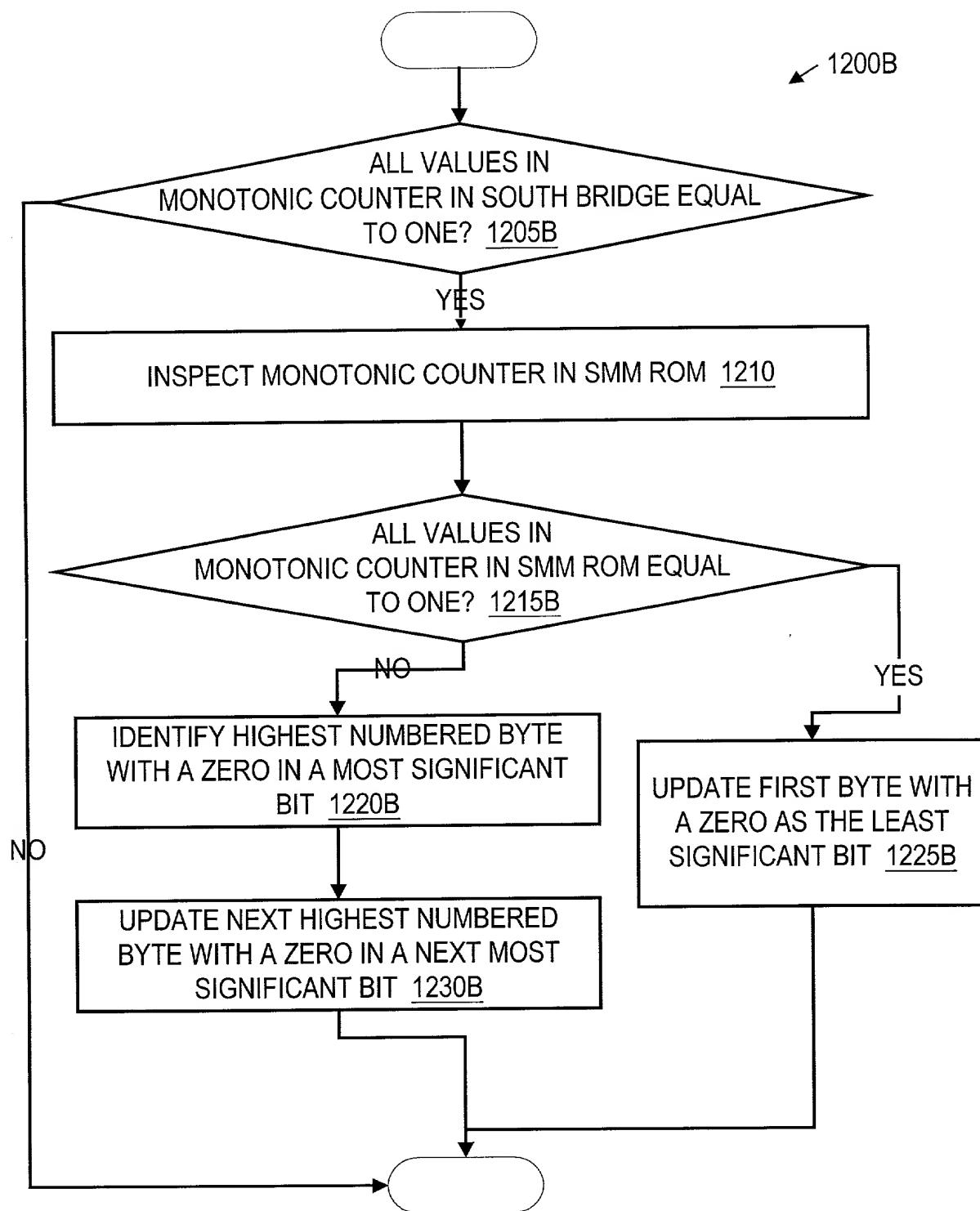


Fig. 12B

23 / 73

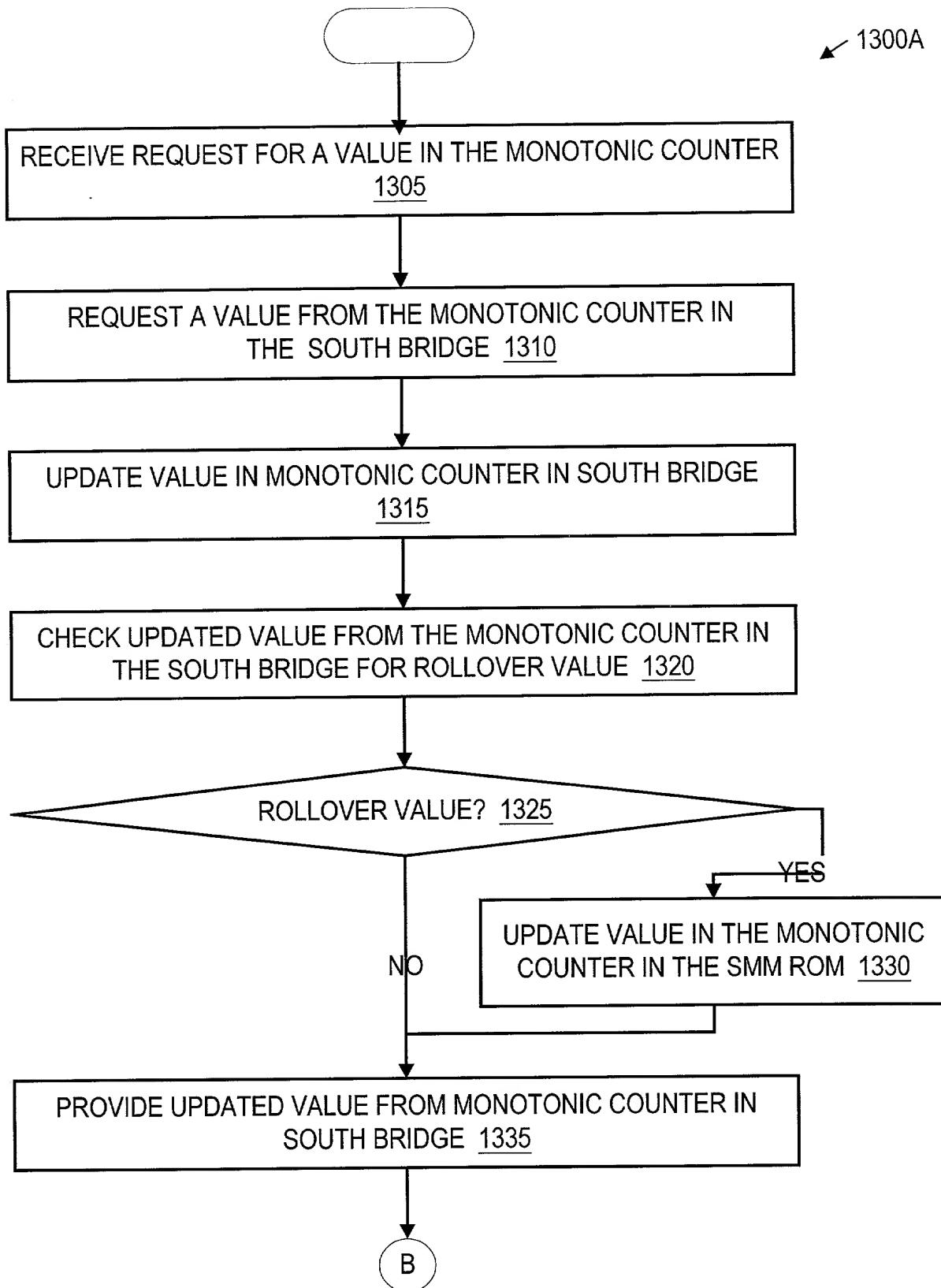


Fig. 13A

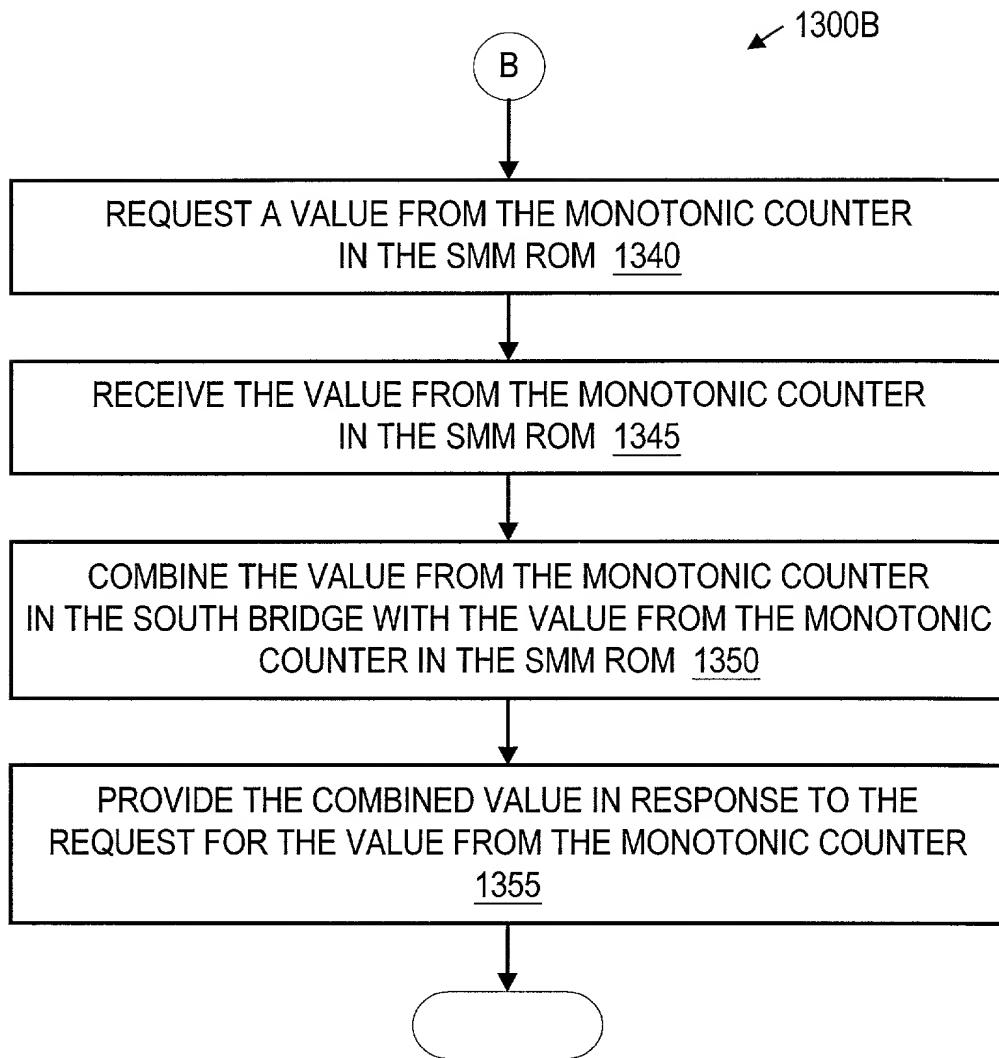


Fig. 13B

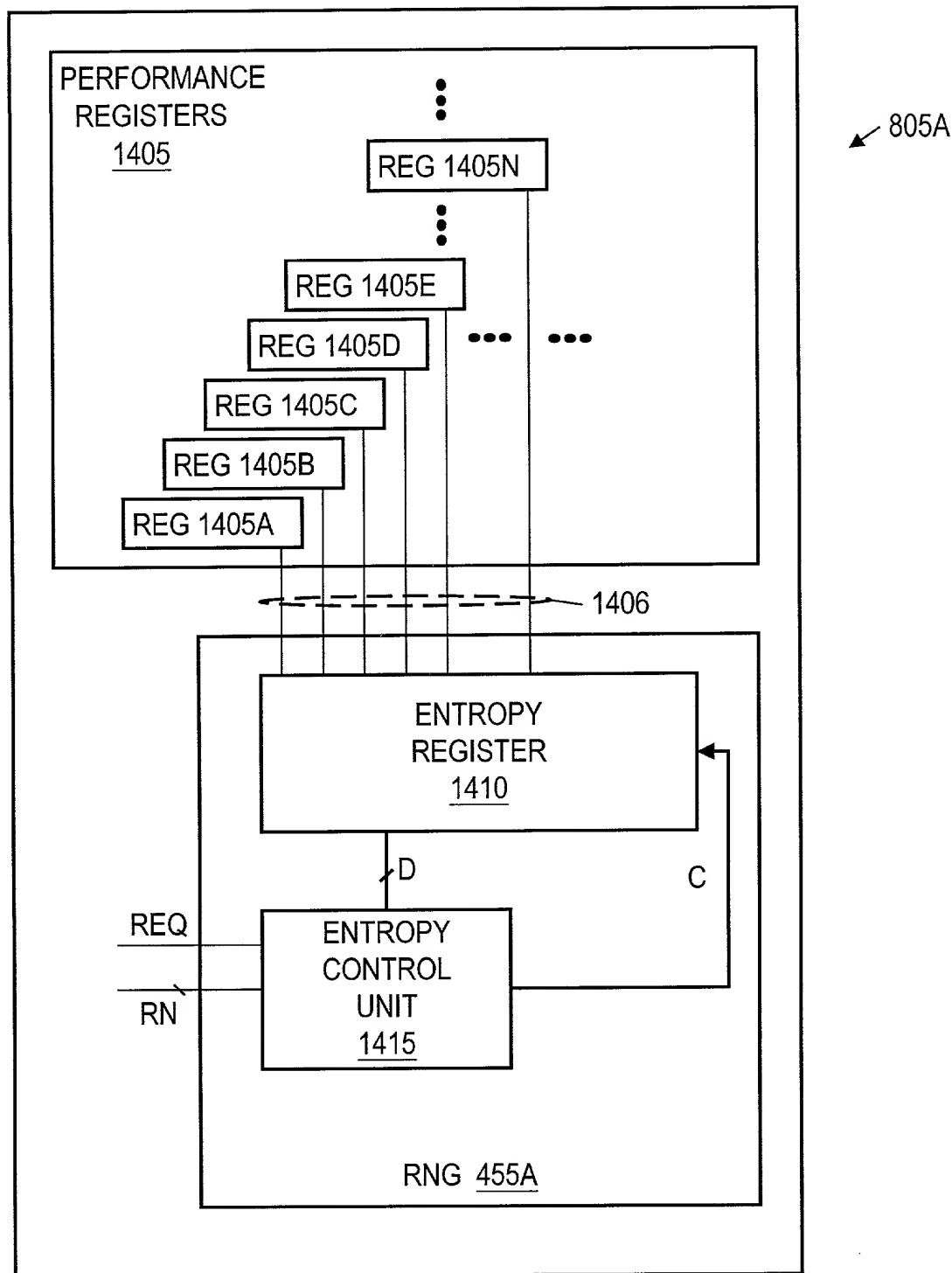


Fig. 14A

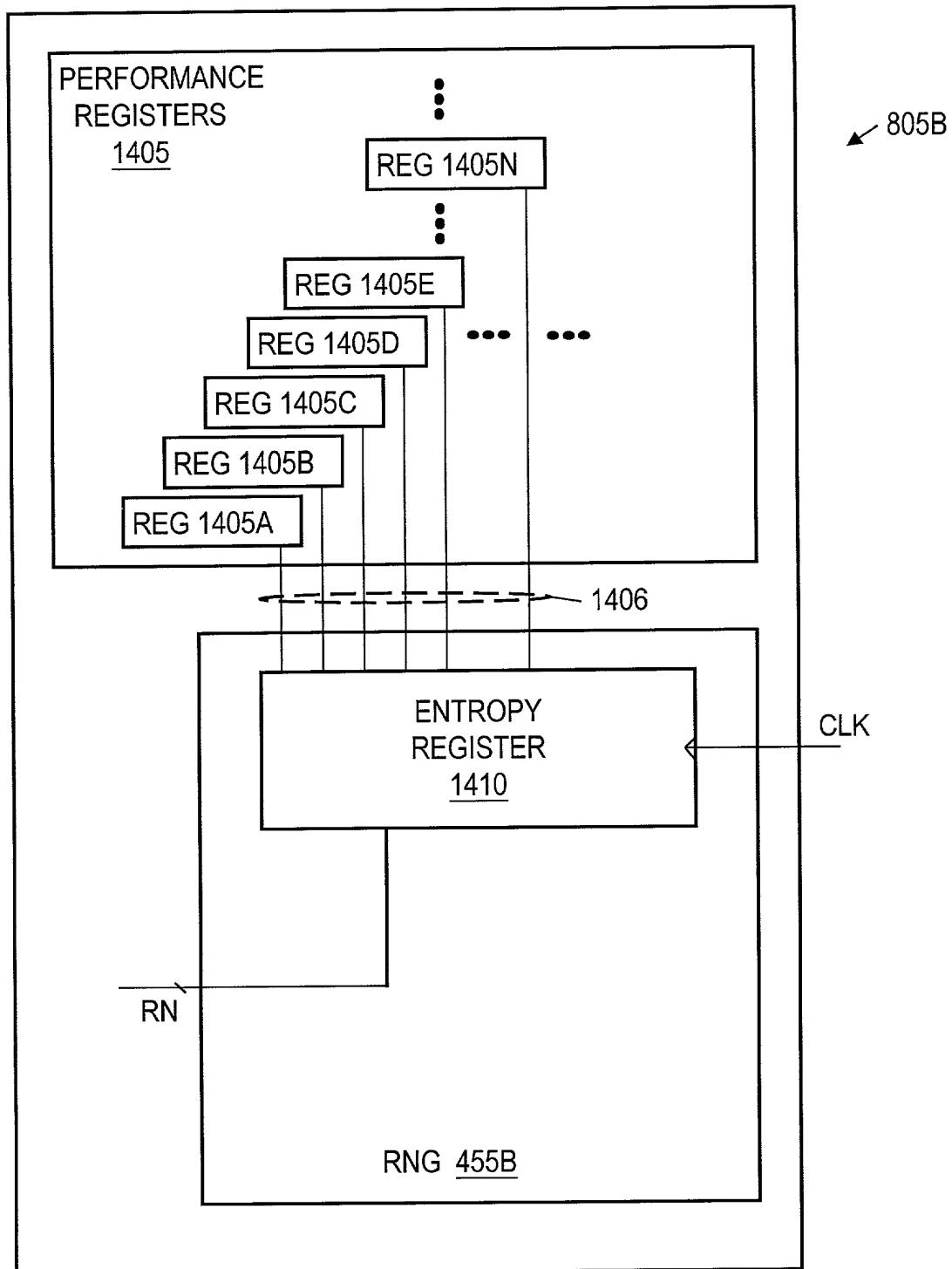


Fig. 14B

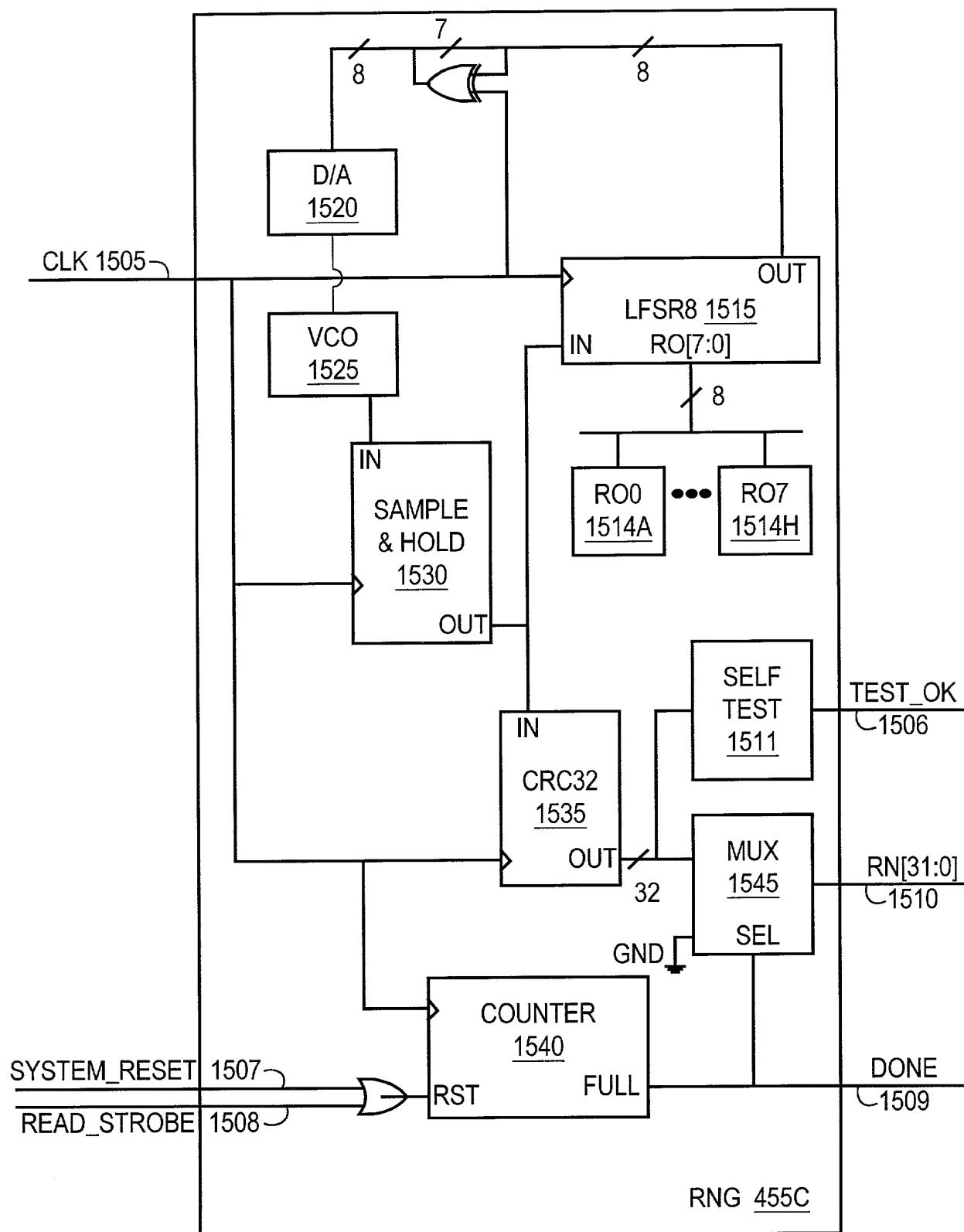


Fig. 15

THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620

BIOS CODE PERFORMS POWER ON SELF TEST (POST) 1625

ACCESSING THE SECURITY HARDWARE 1630

OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632

BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635

BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 1640

BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645

CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

BIOS CODE IDENTIFIES THE BOOT LOCATION 1655

BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16A

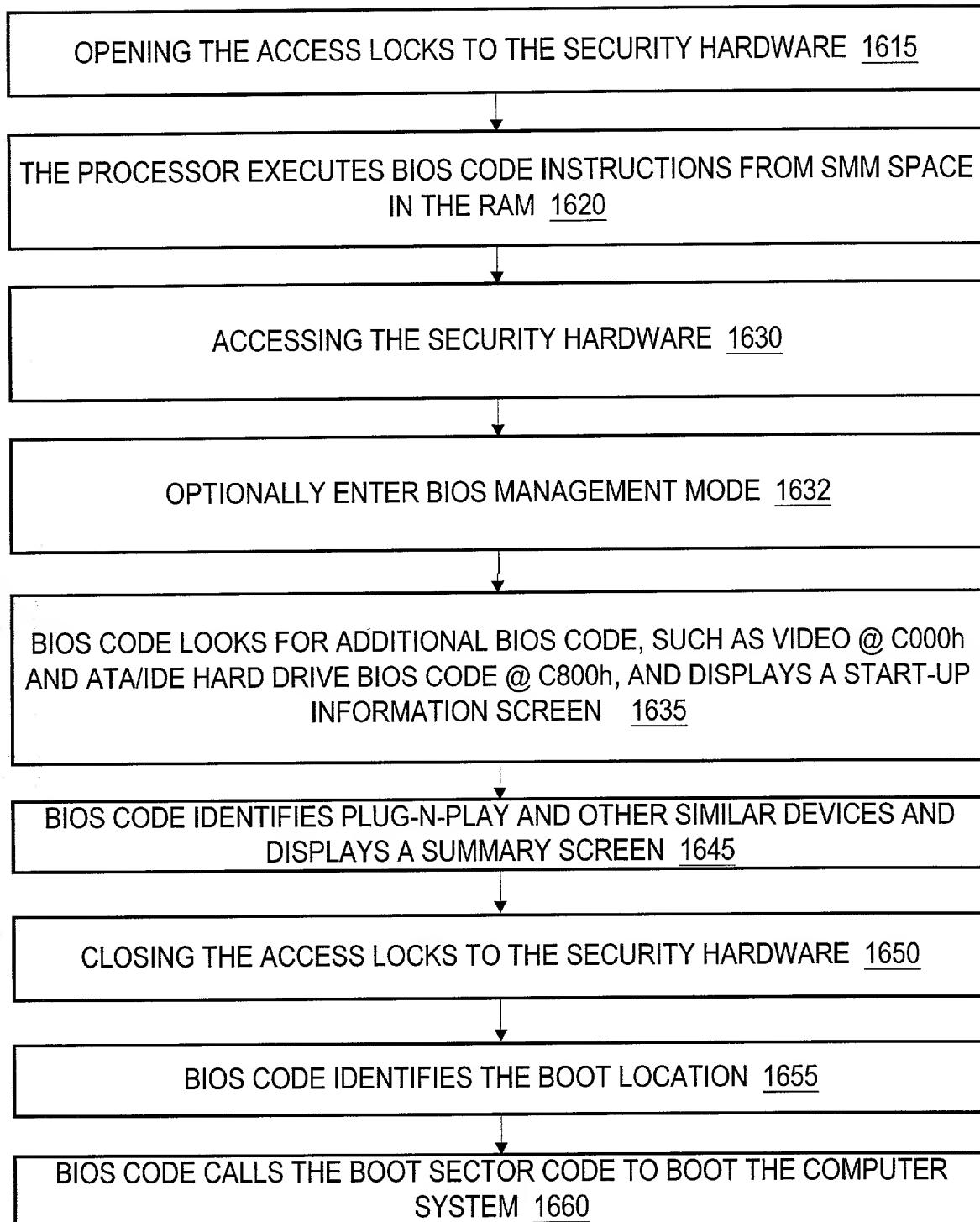


Fig. 16B

30 / 73

1600C

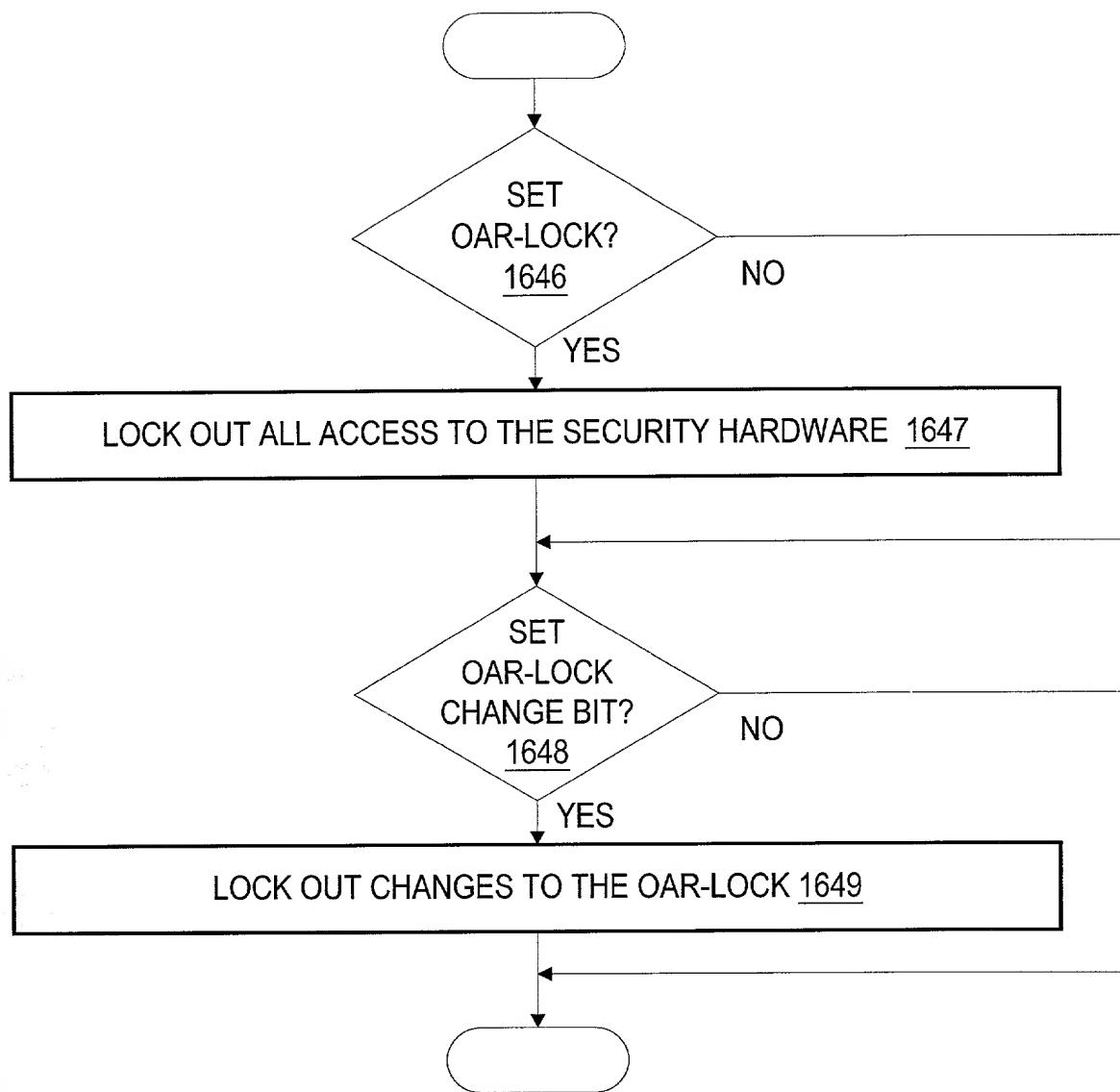


Fig. 16C

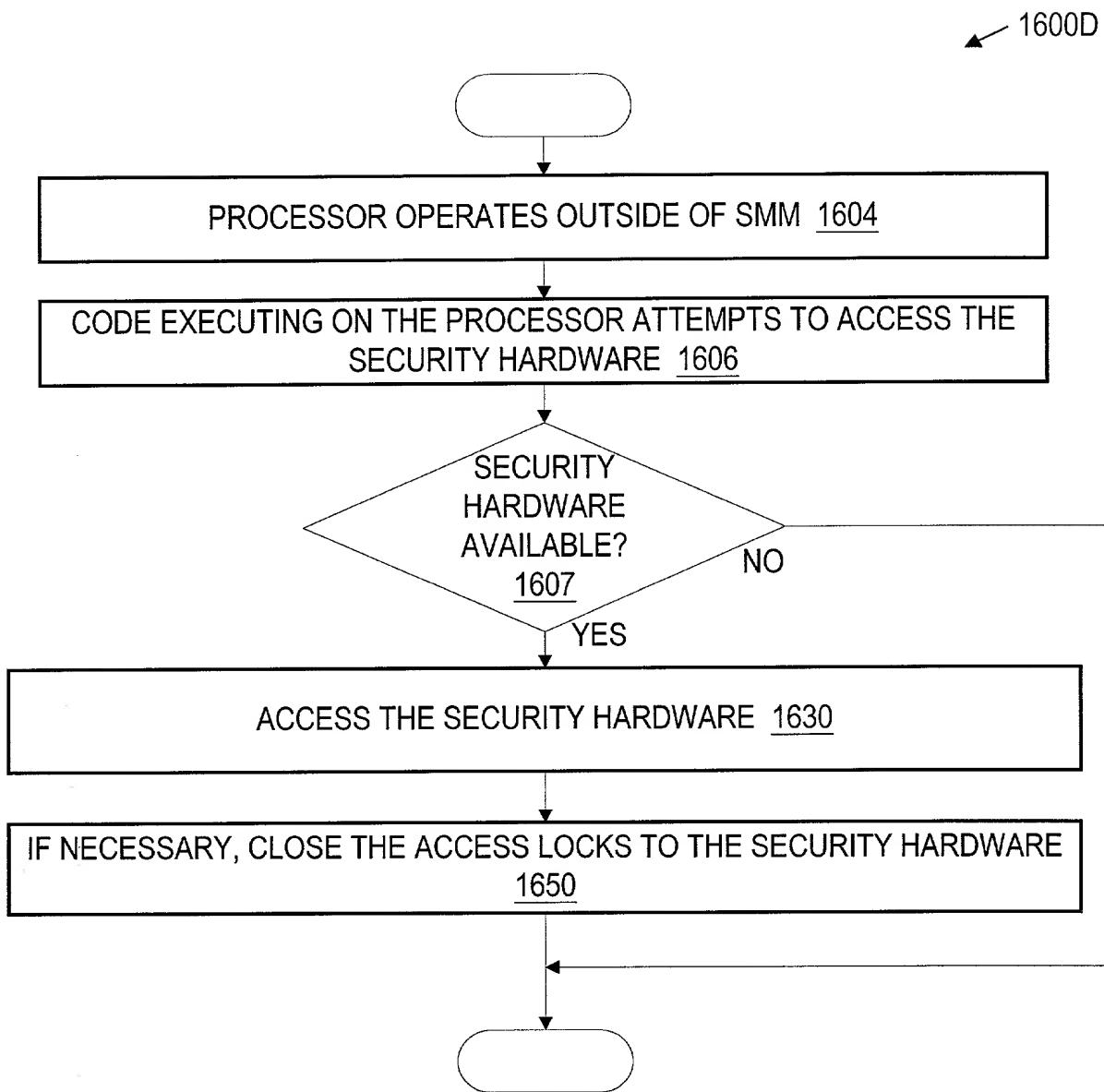


Fig. 16D

32 / 73

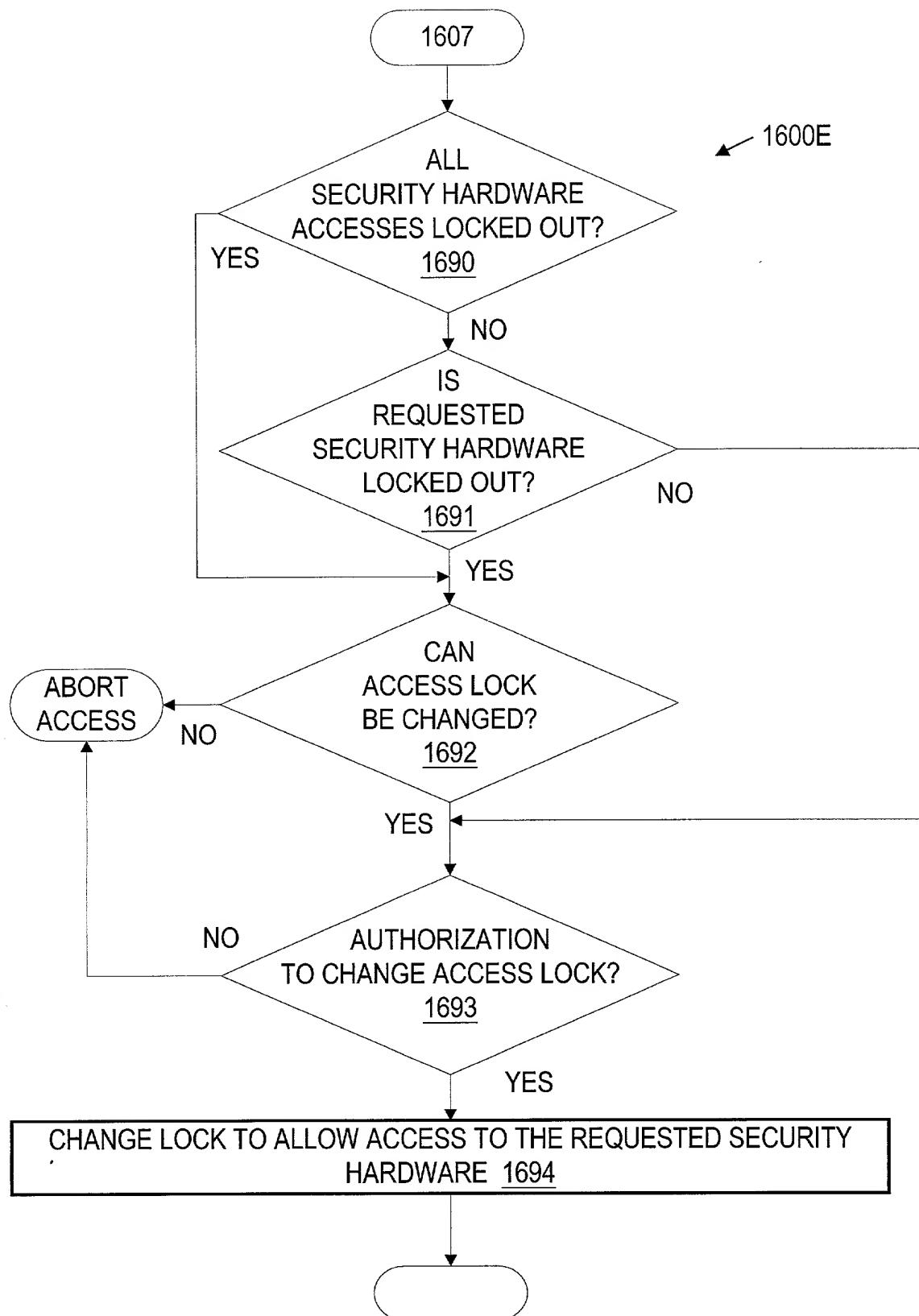
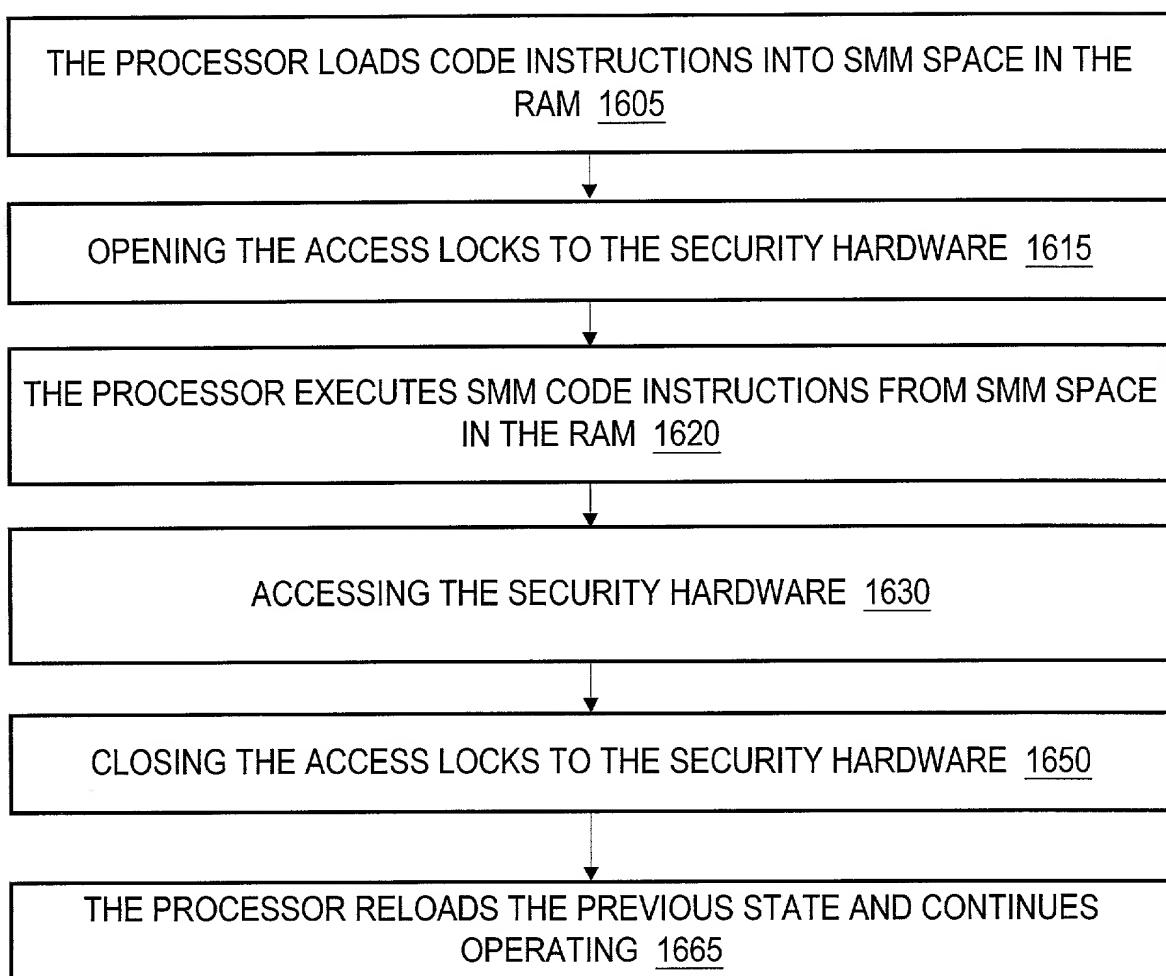
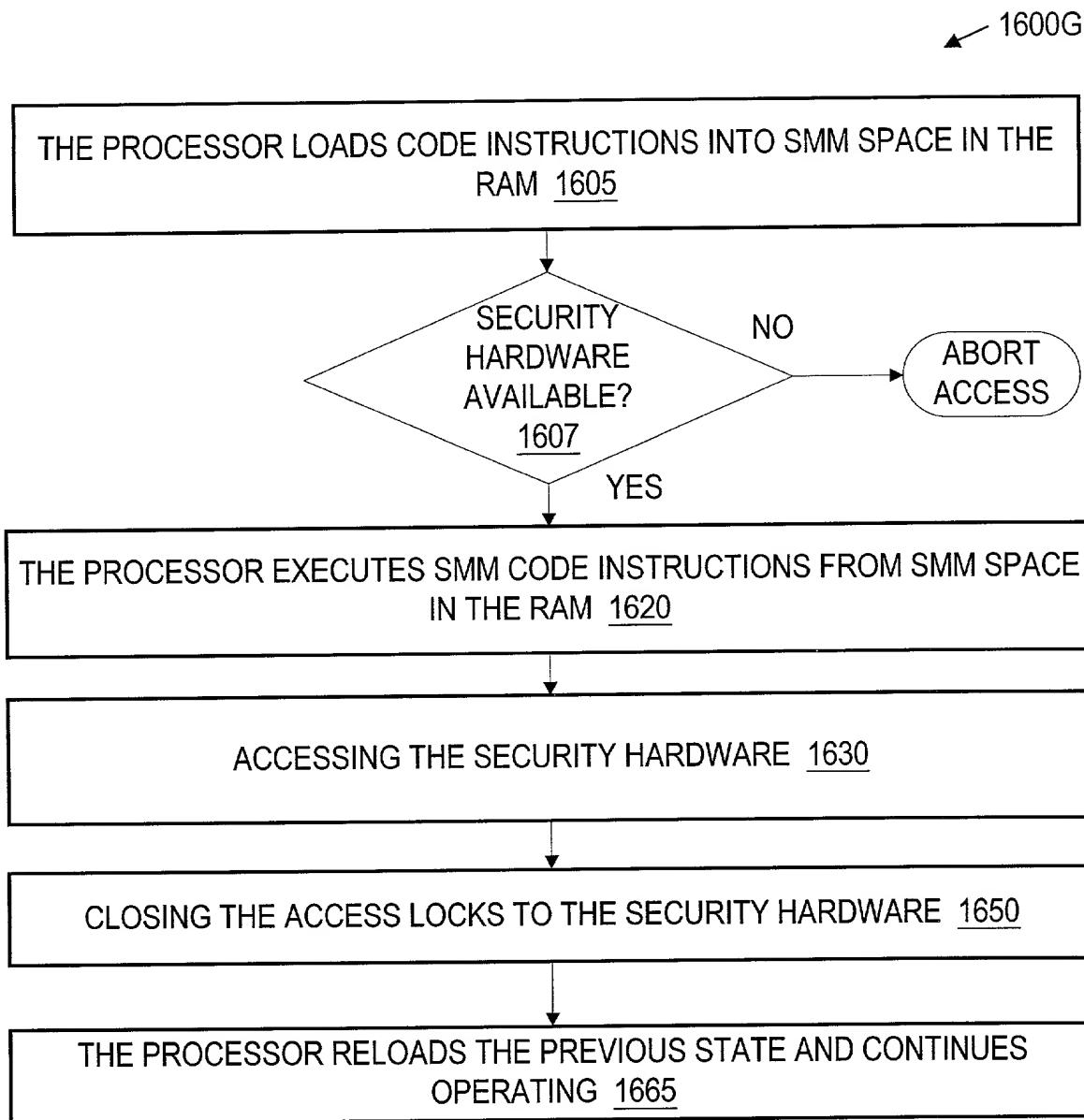


Fig. 16E



1600F

09853226 054103



1600G

Fig. 16G

35 / 73

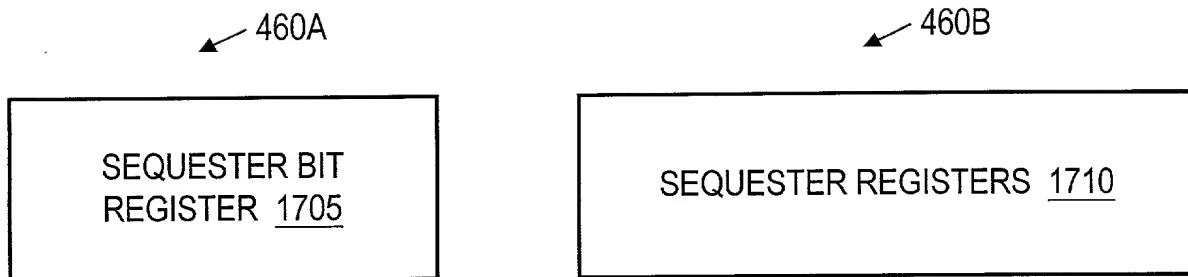


Fig. 17A

Fig. 17B

092252226 0924404

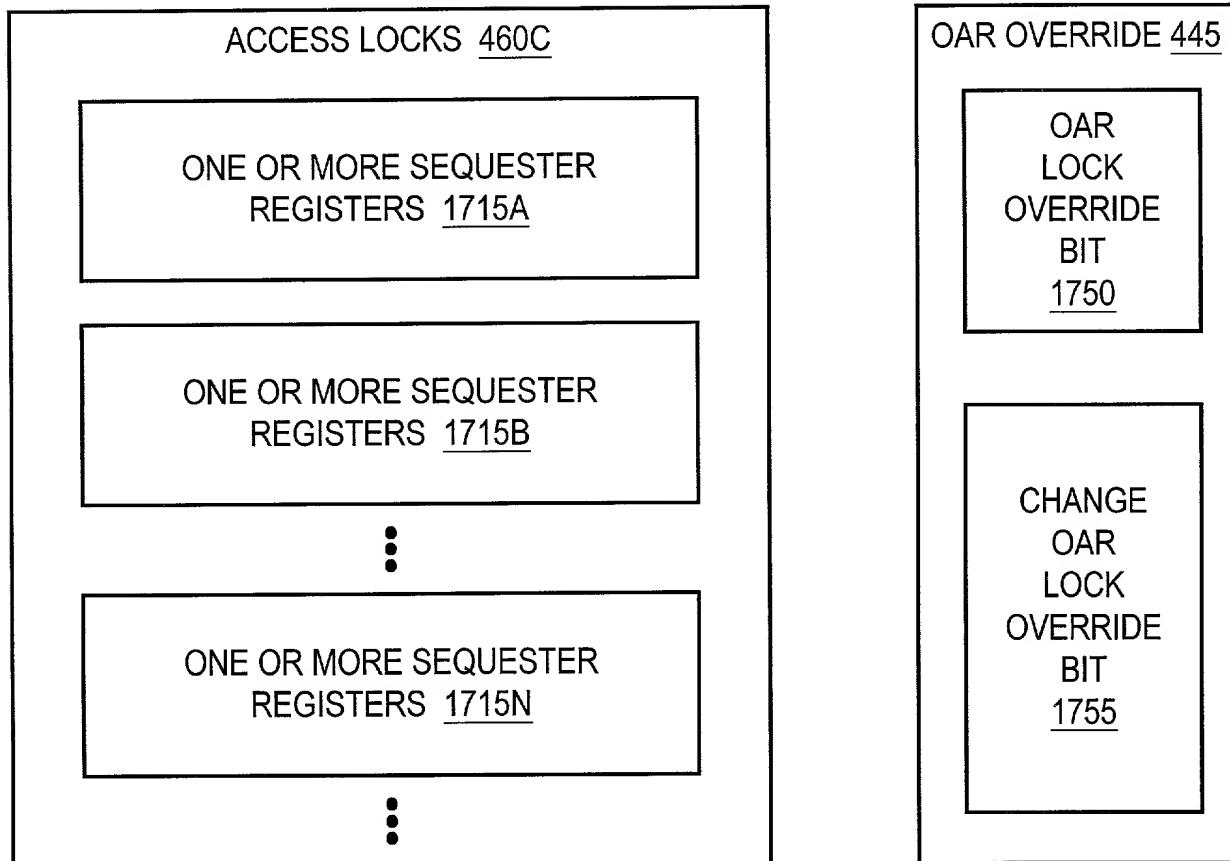


Fig. 17C

Fig. 17D

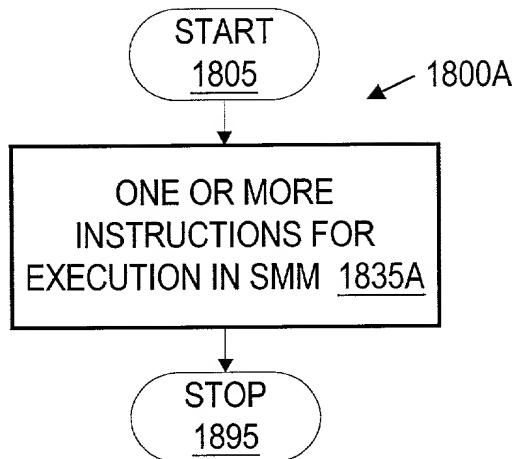


Fig. 18A
PRIOR ART

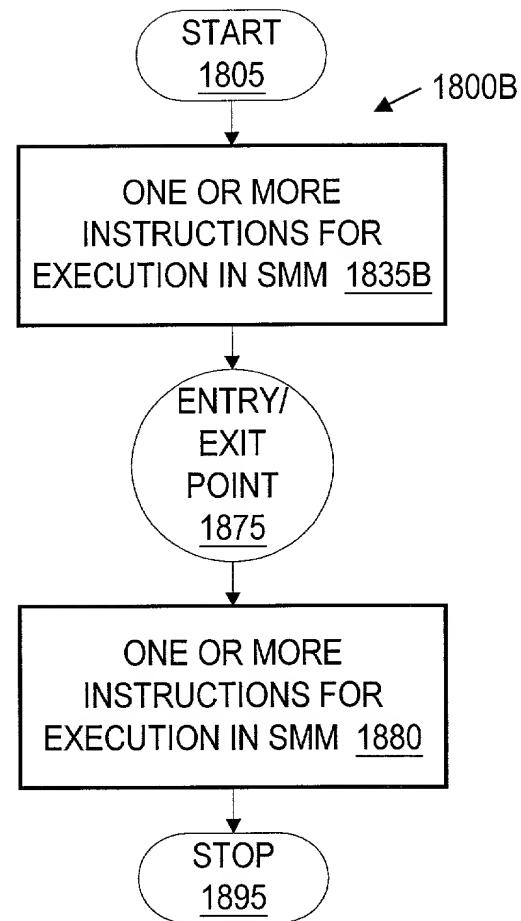


Fig. 18B

37 / 73

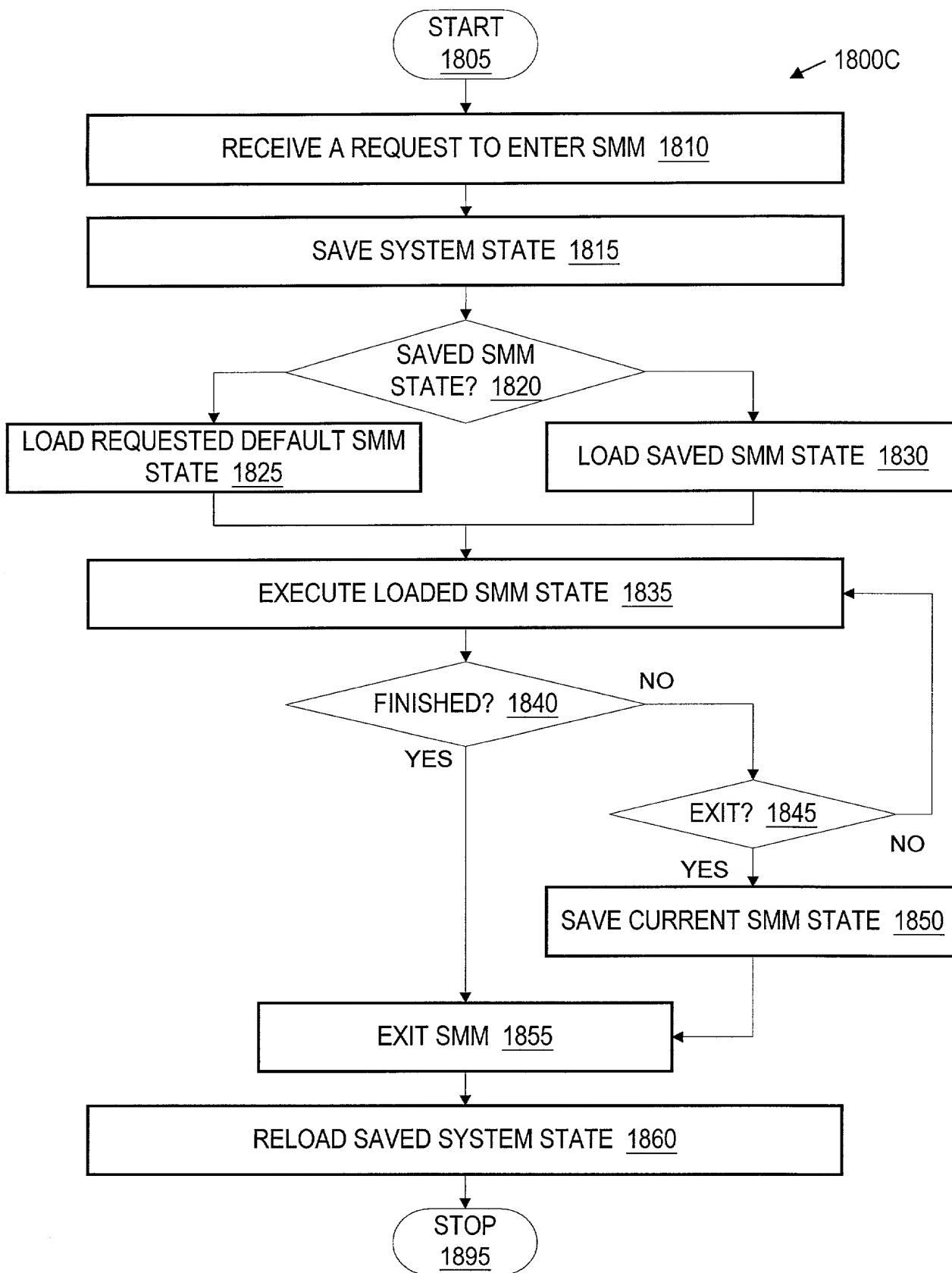


Fig. 18C

38 / 73

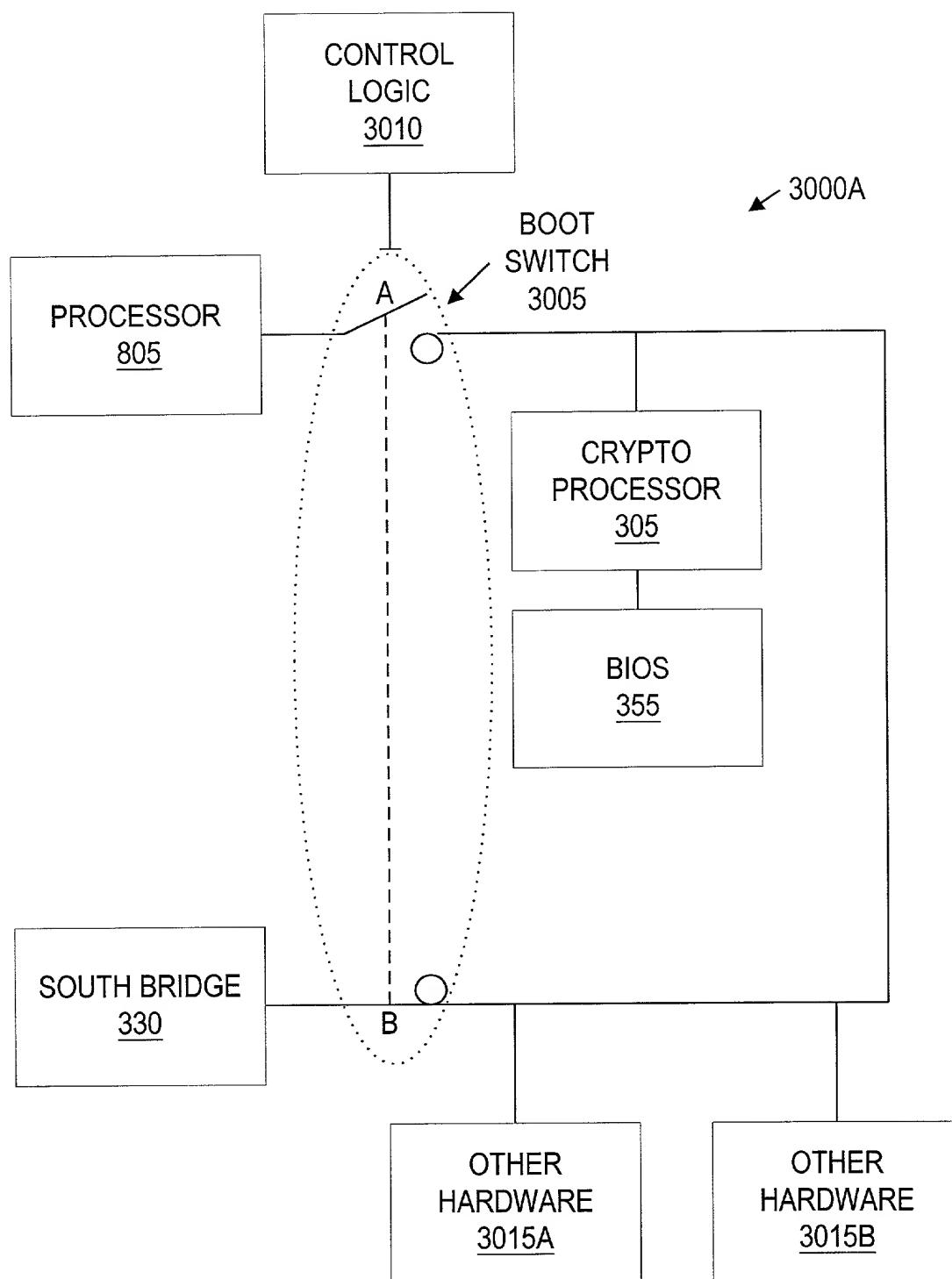
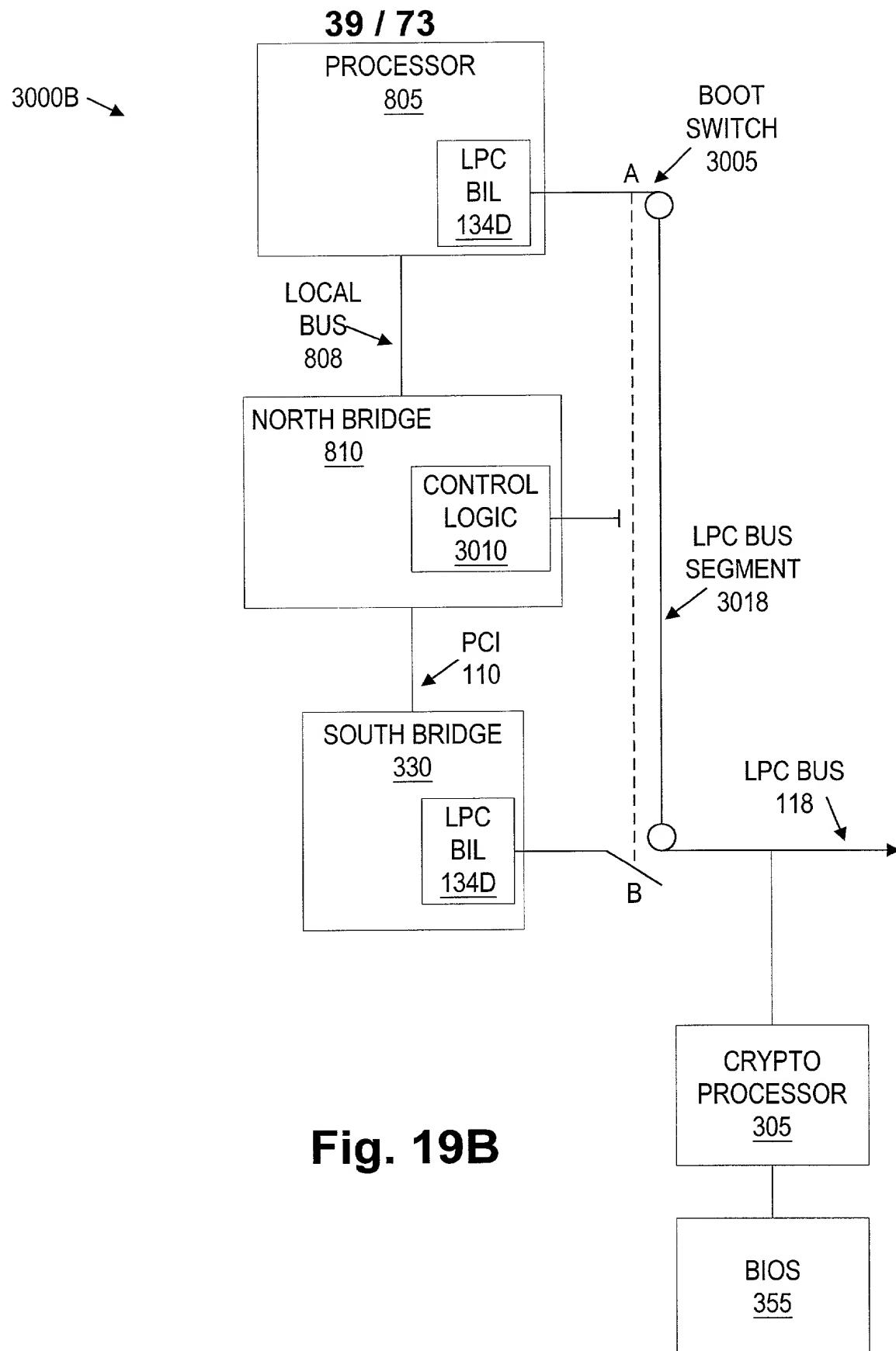
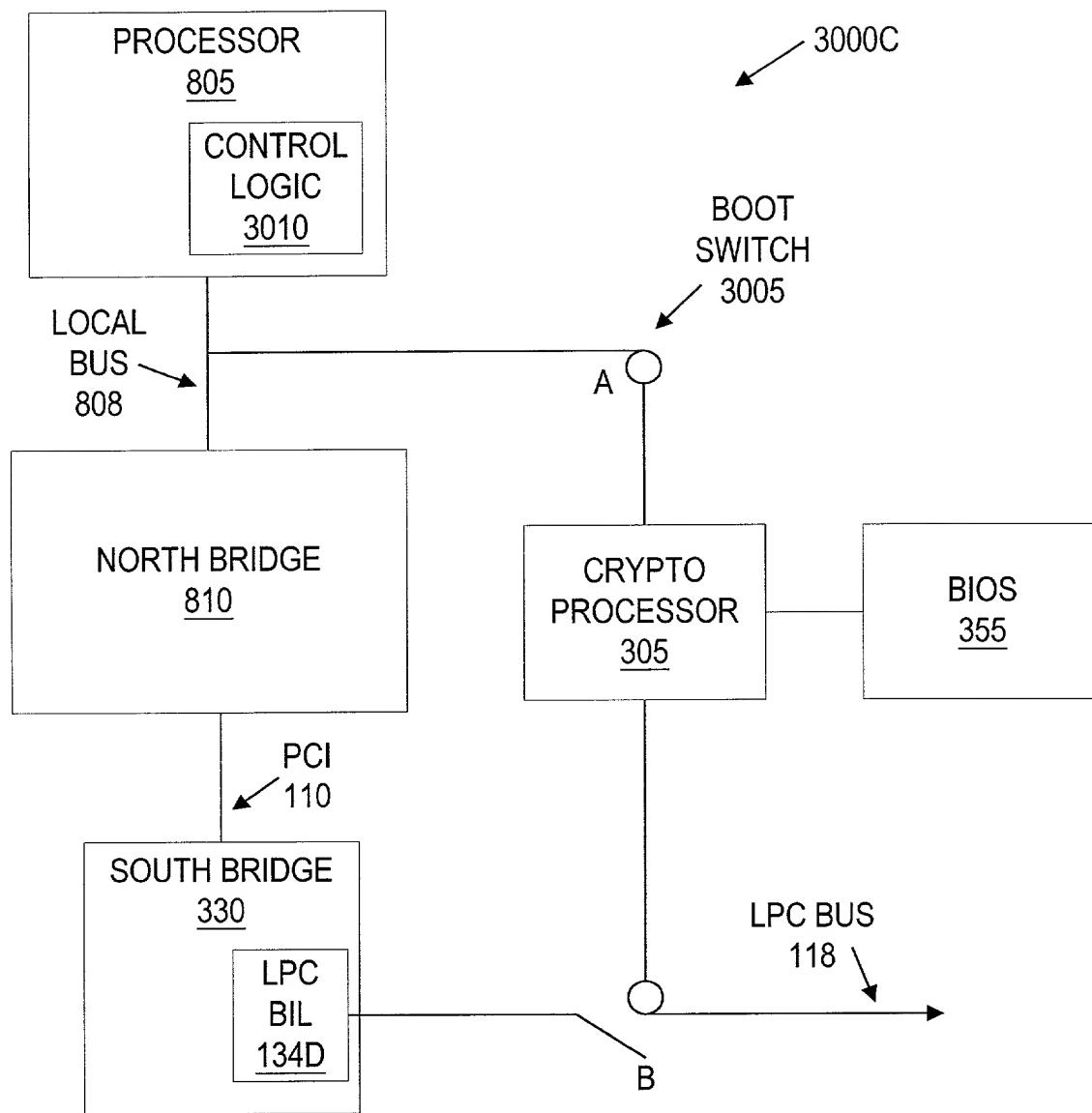


Fig. 19A



**Fig. 19C**

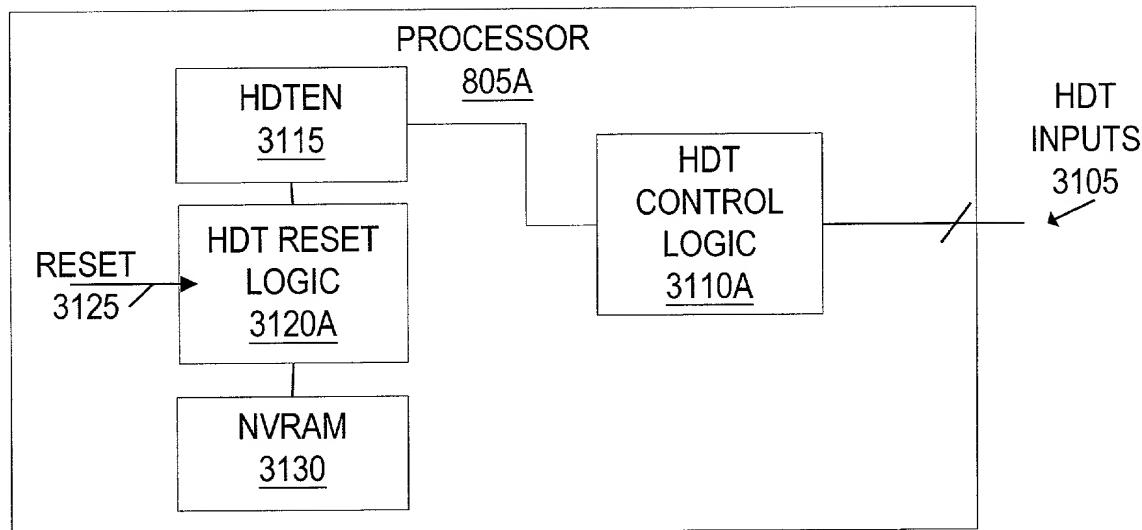


Fig. 20A

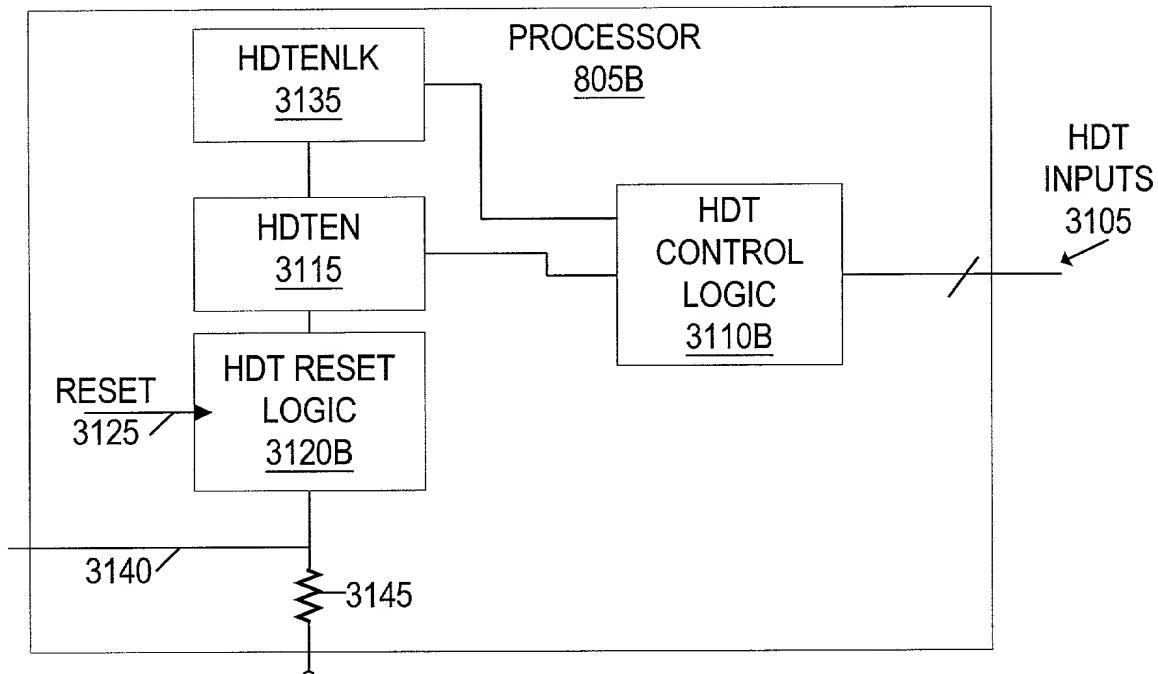
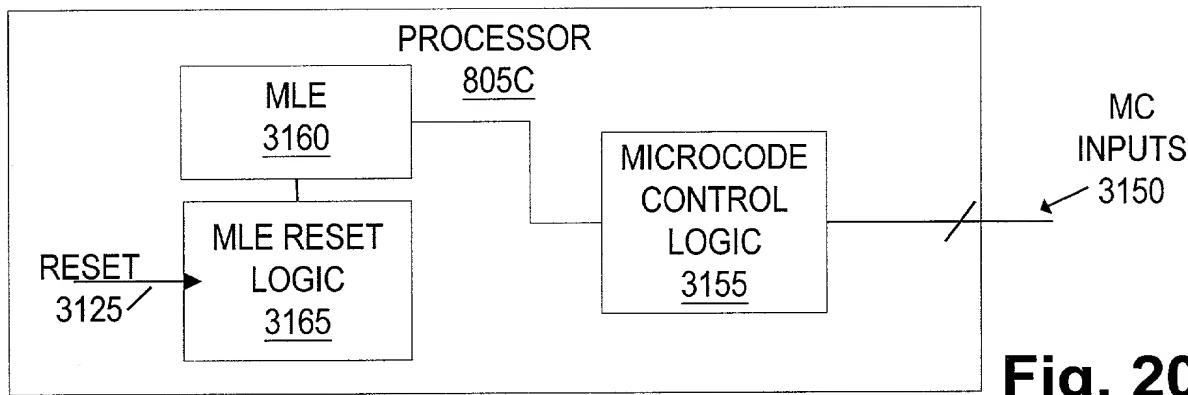
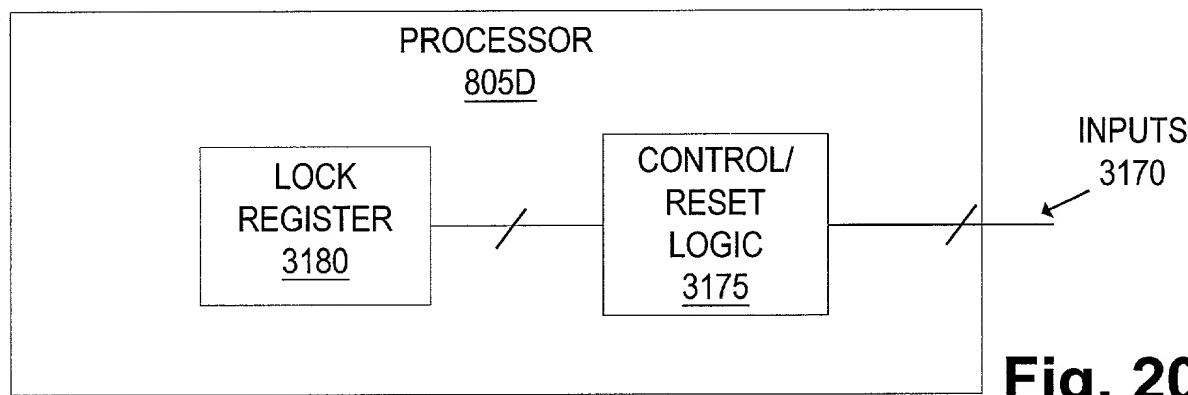


Fig. 20B

42 / 73

**Fig. 20C****Fig. 20D**

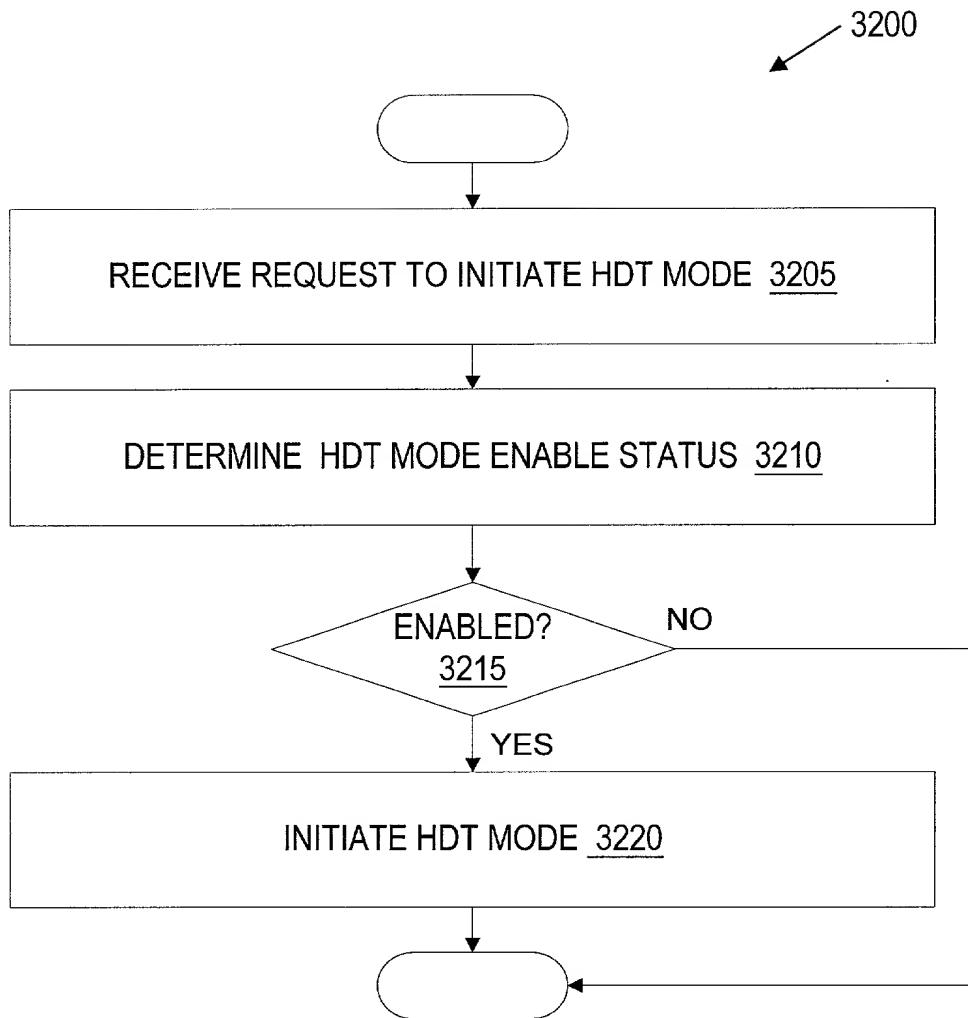


Fig. 21

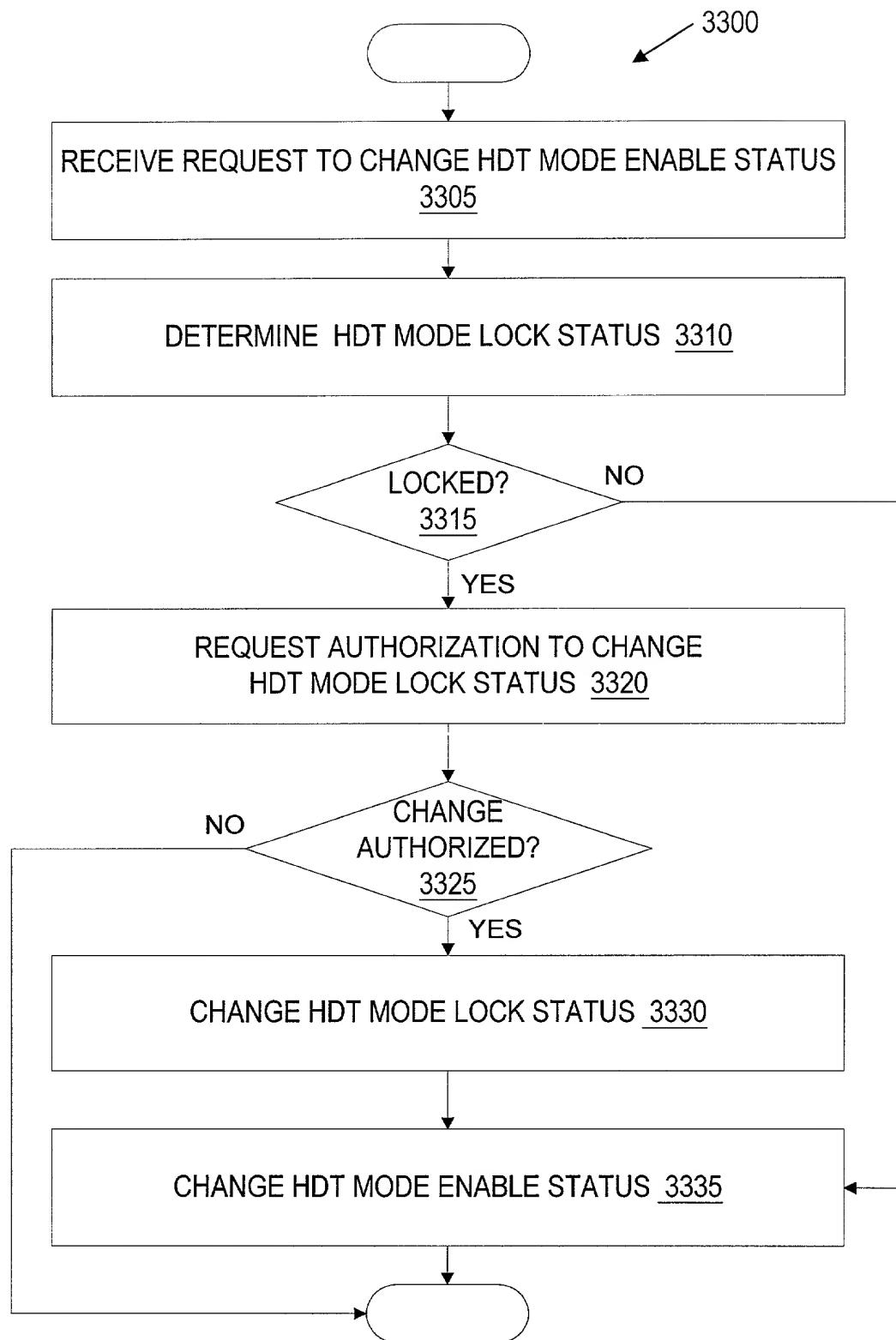
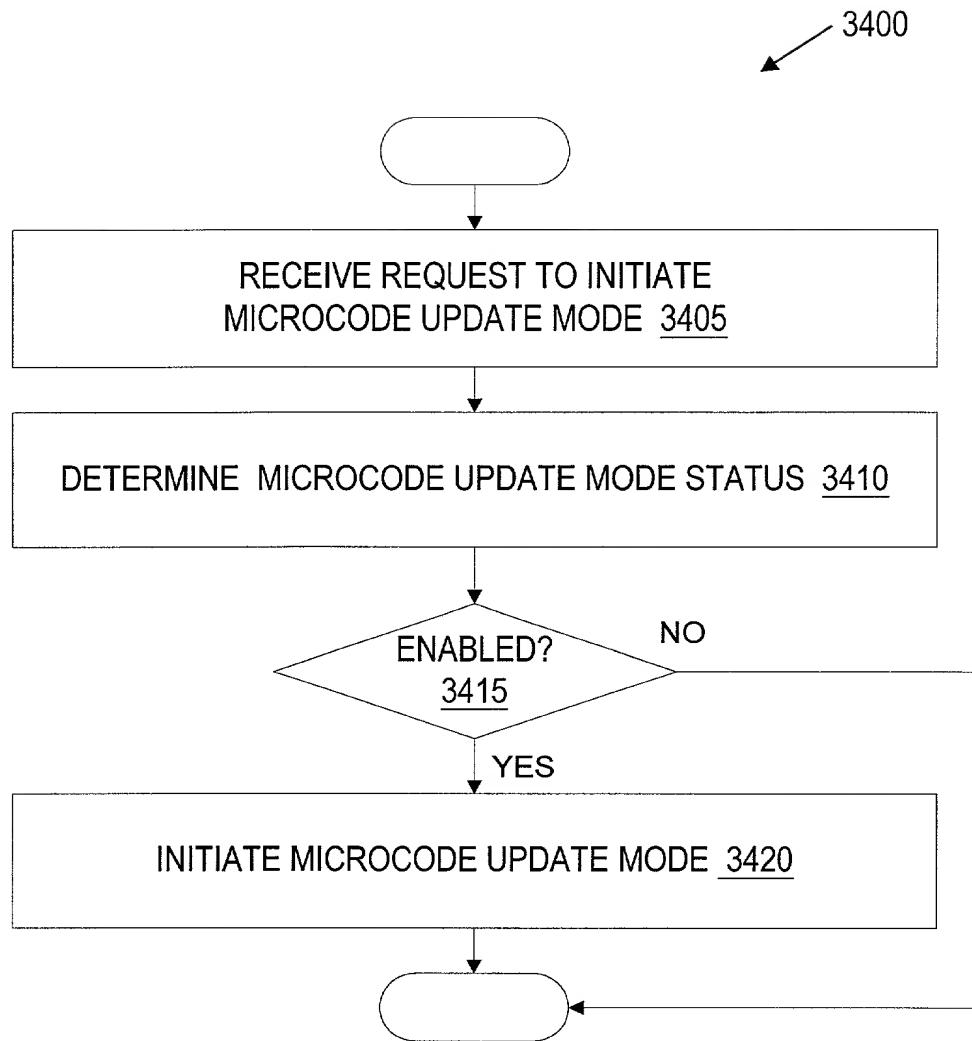


Fig. 22

**Fig. 23**

46 / 73

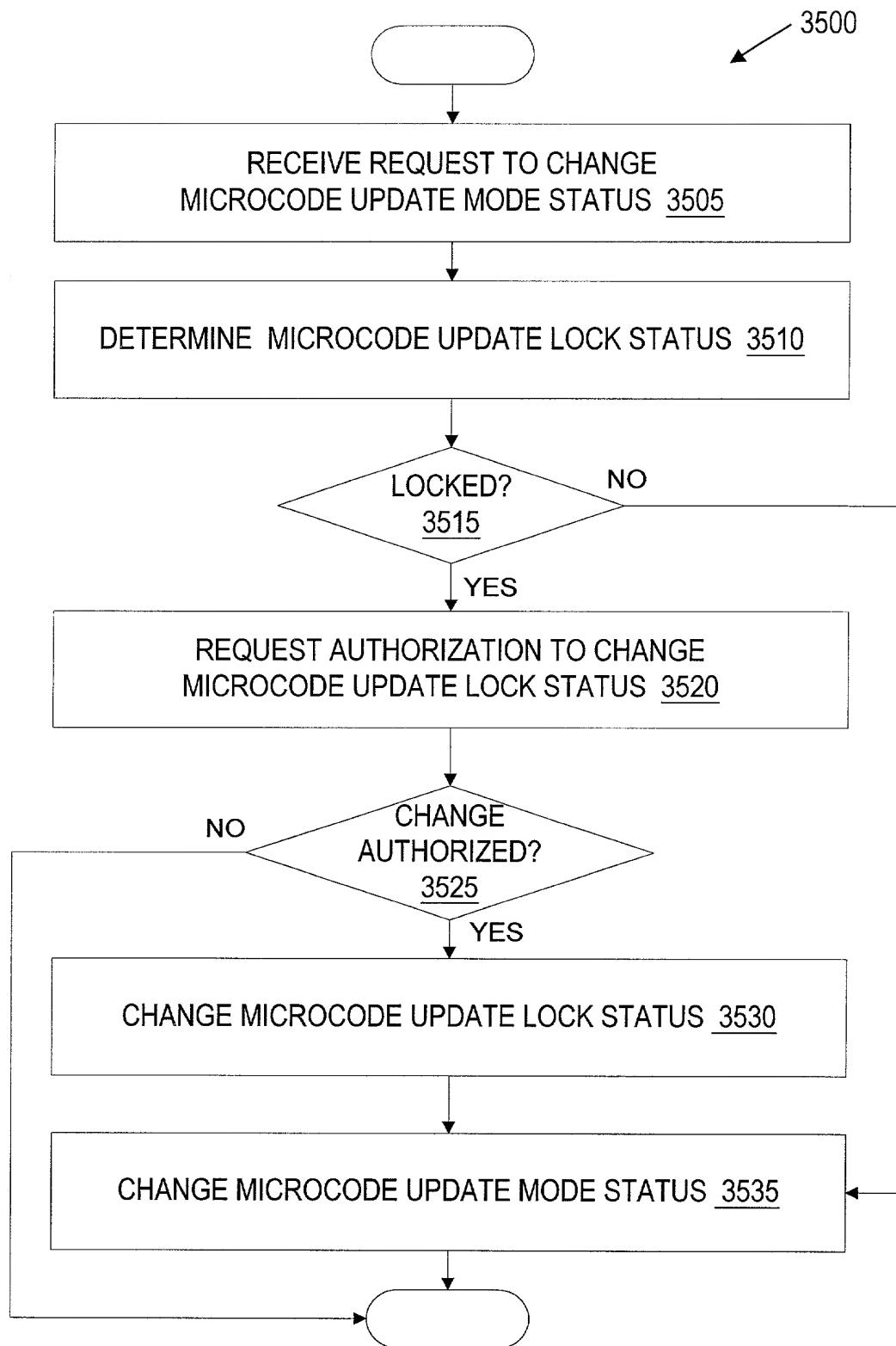
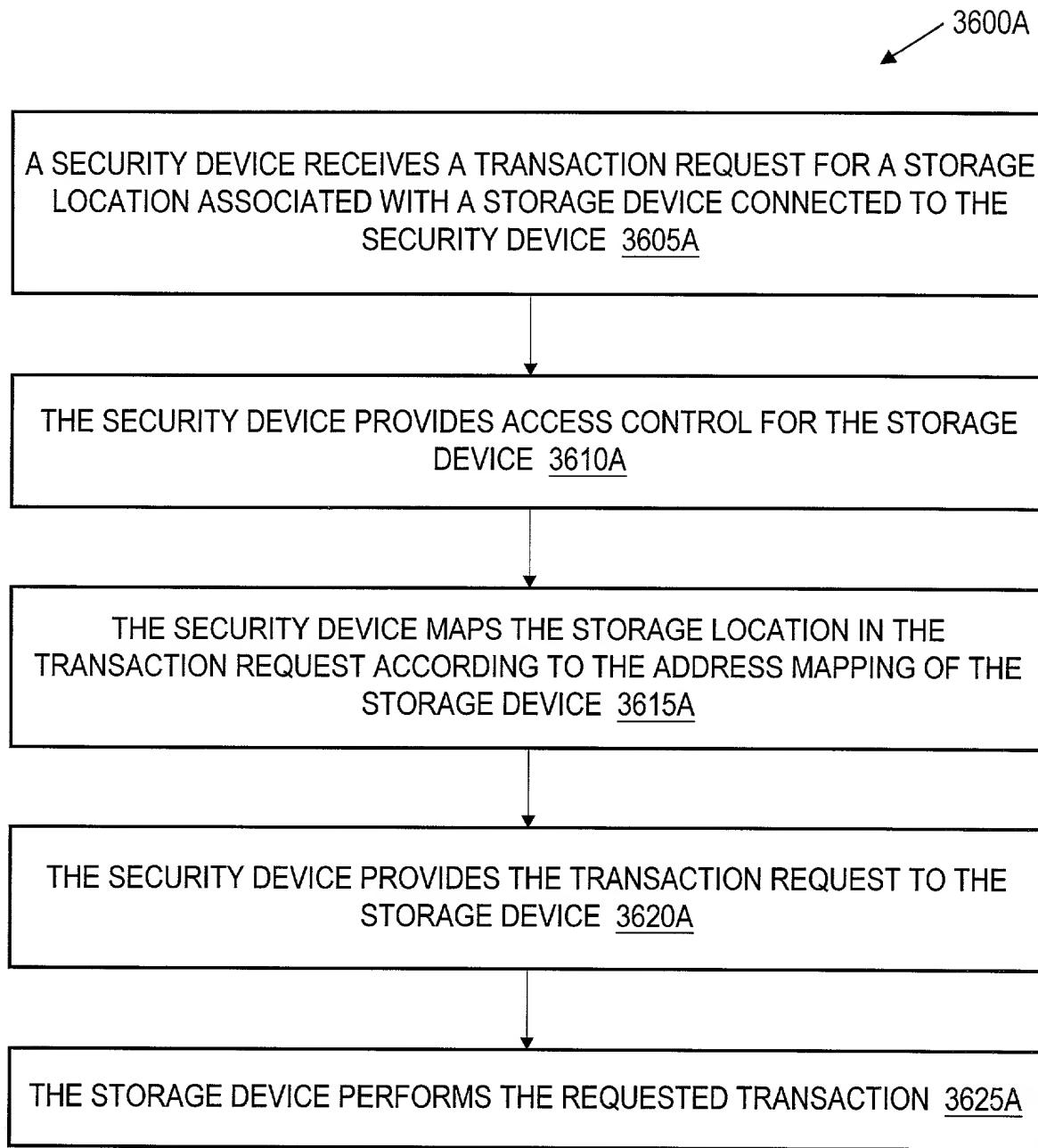


Fig. 24



3600A

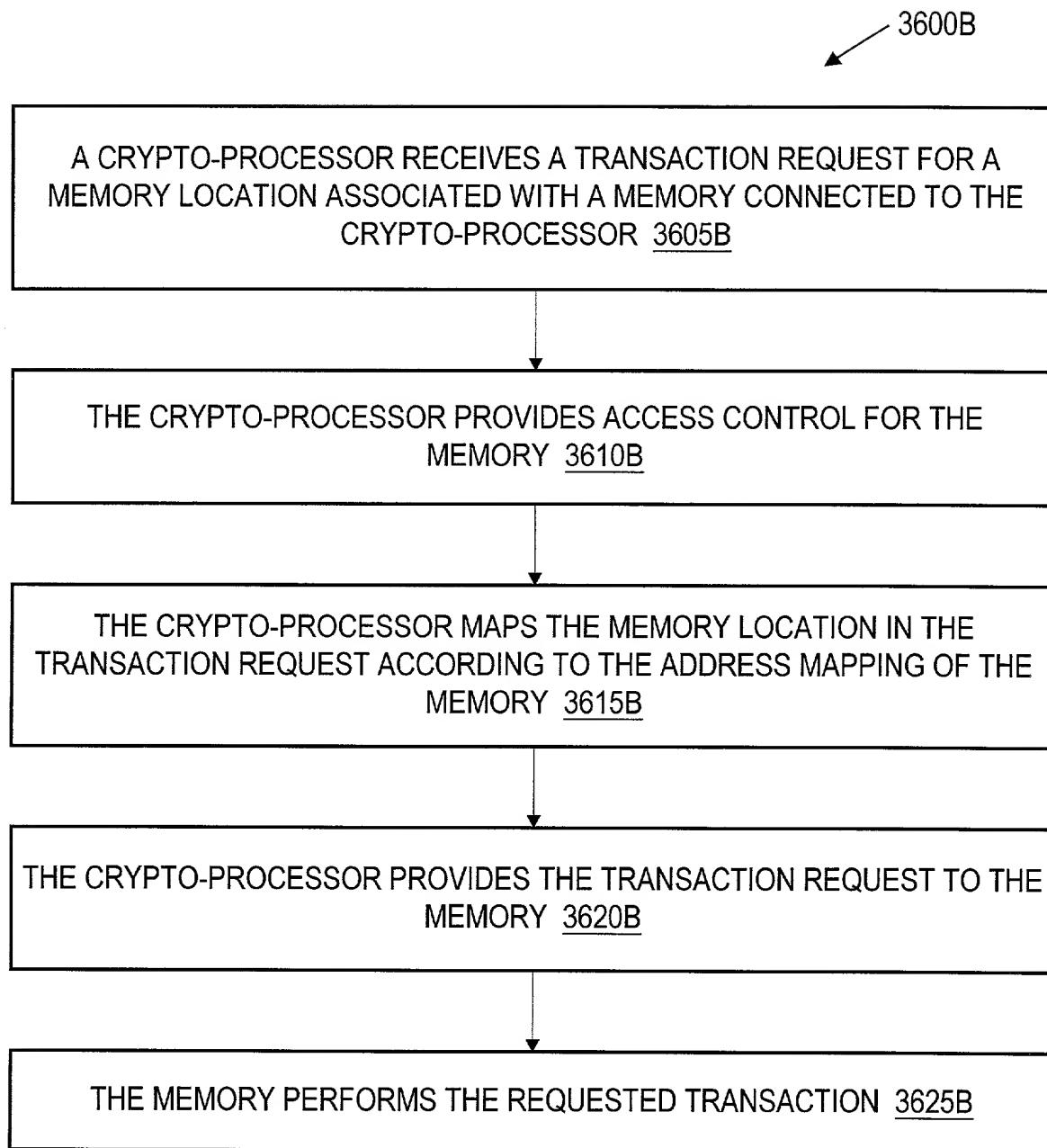


Fig. 25B

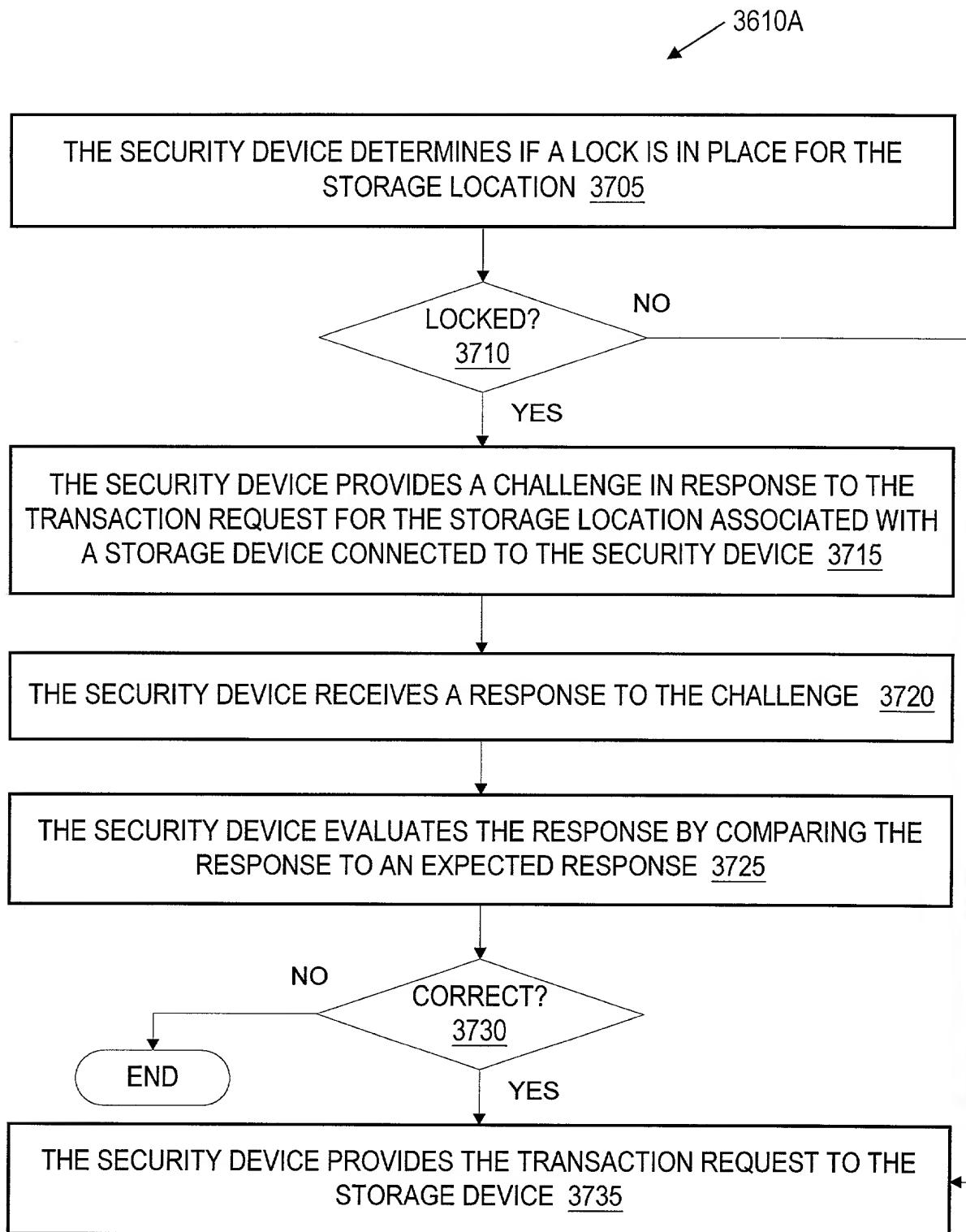


Fig. 26

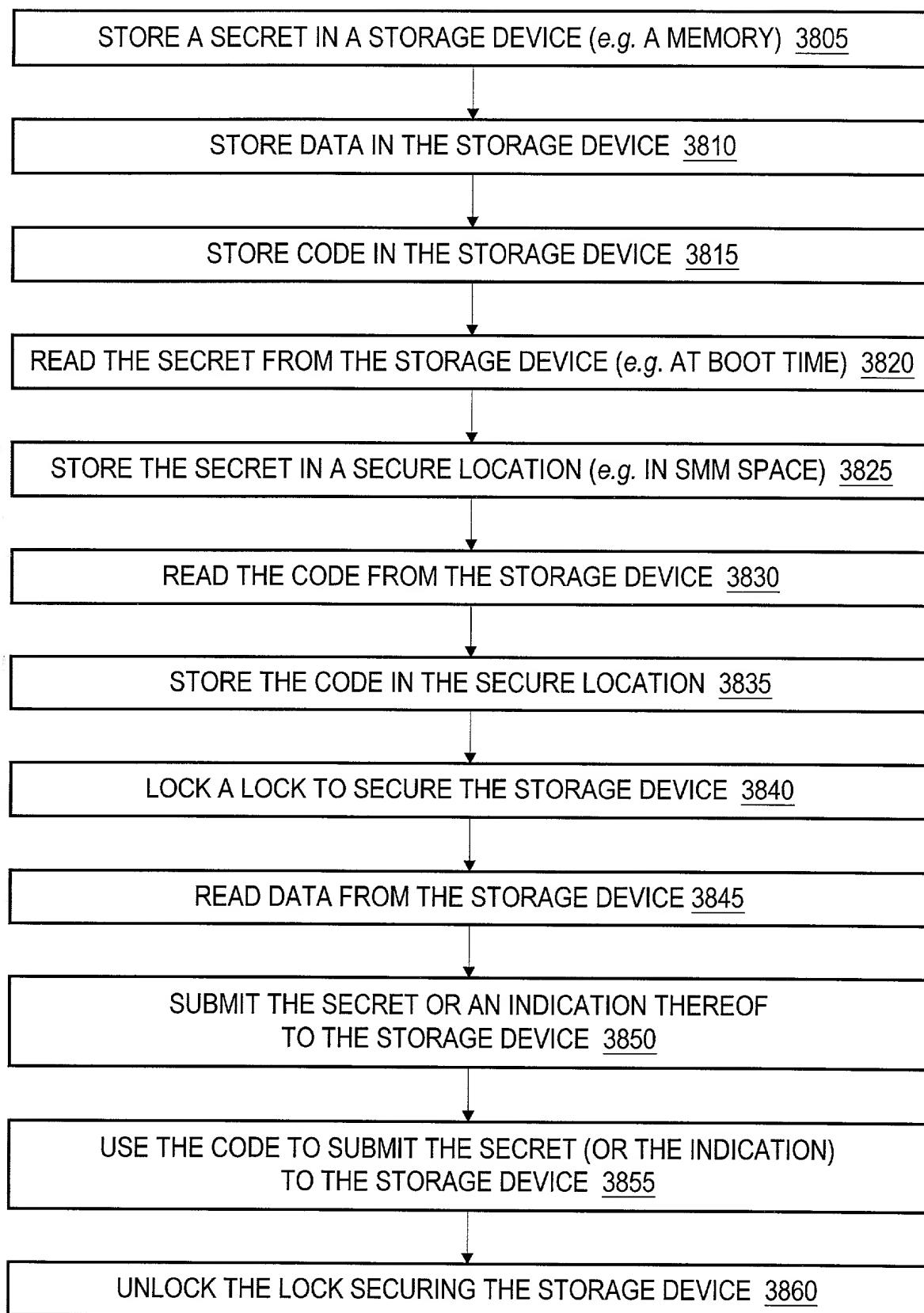


Fig. 27

51 / 73

3900

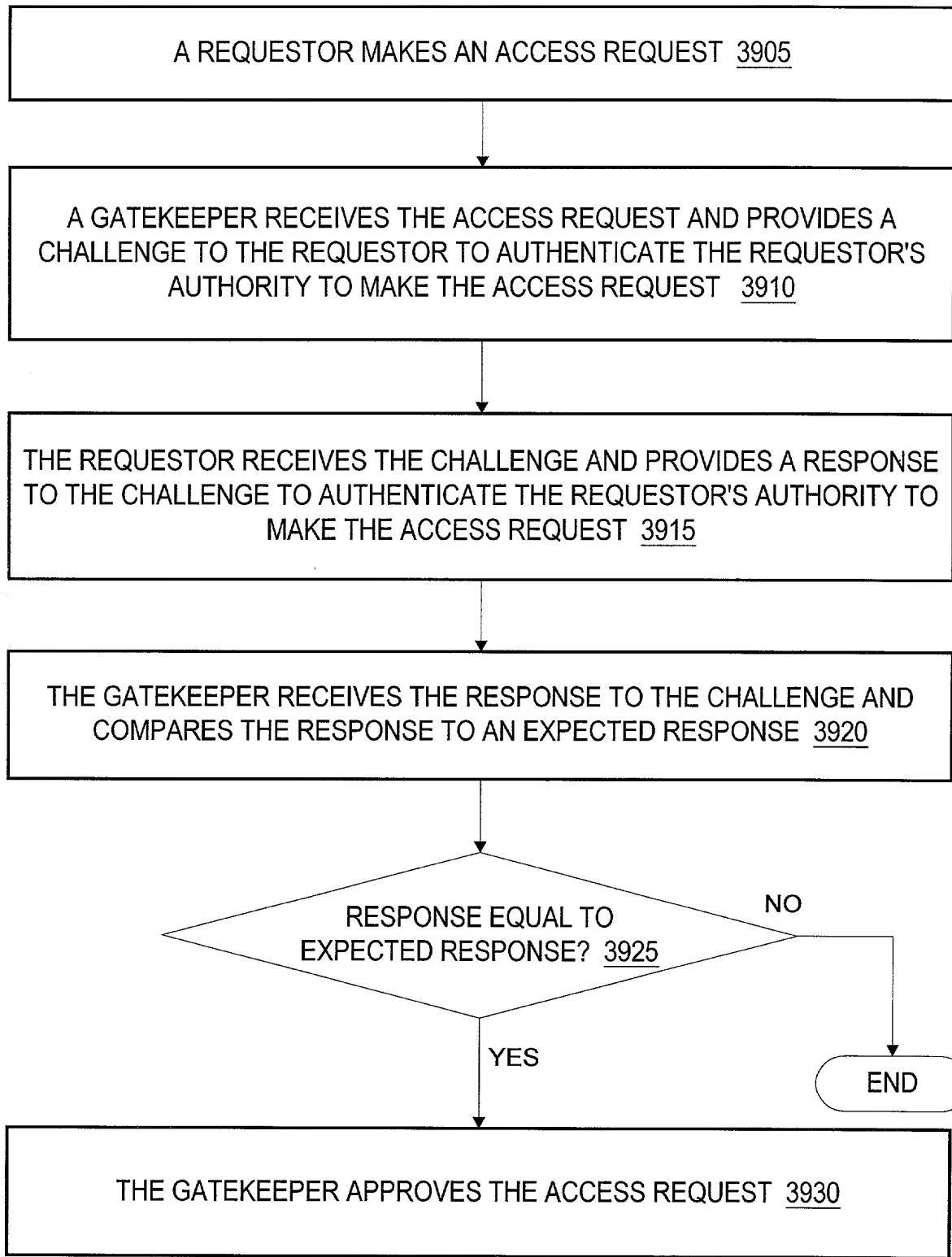


Fig. 28
(Prior Art)

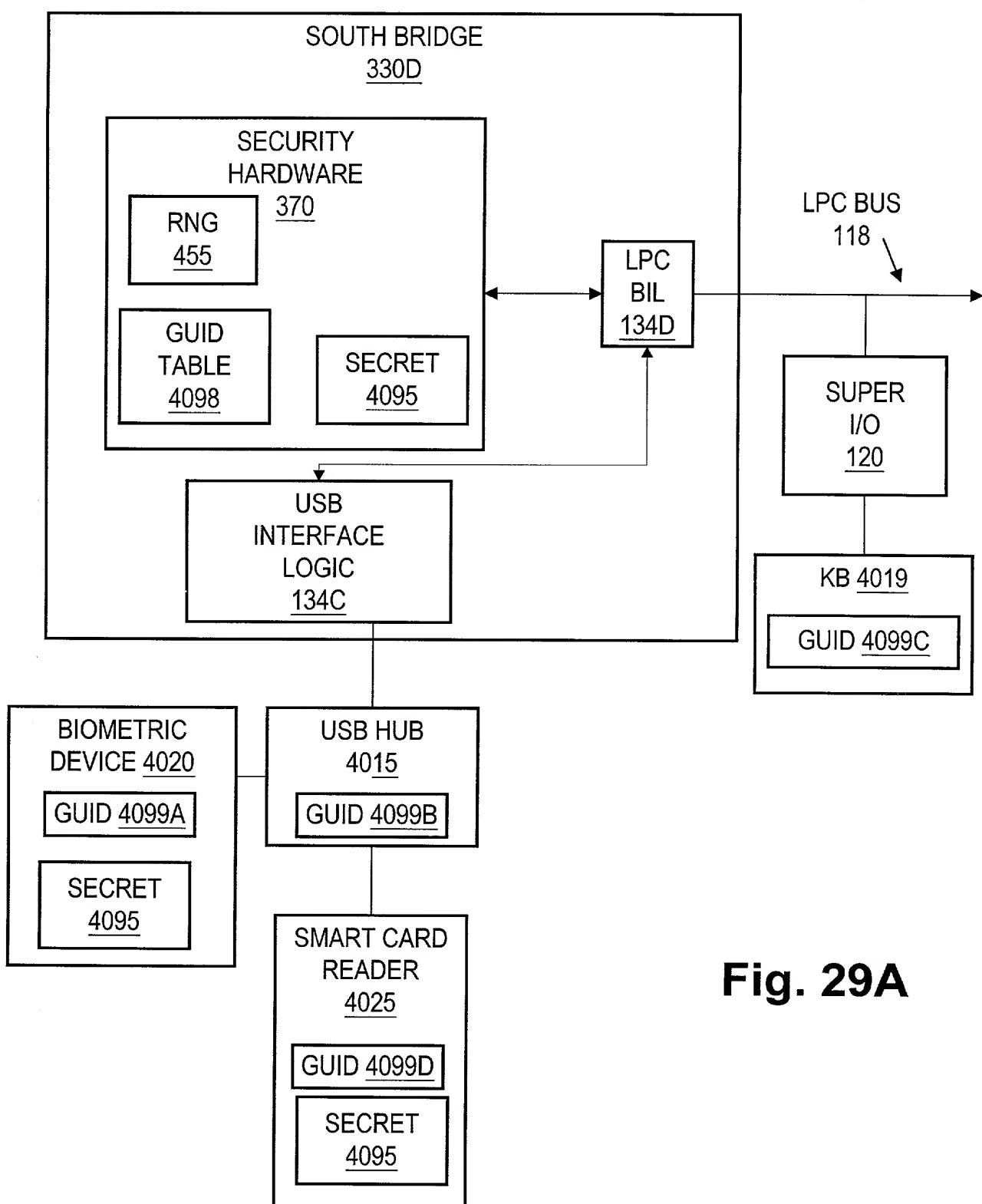


Fig. 29A

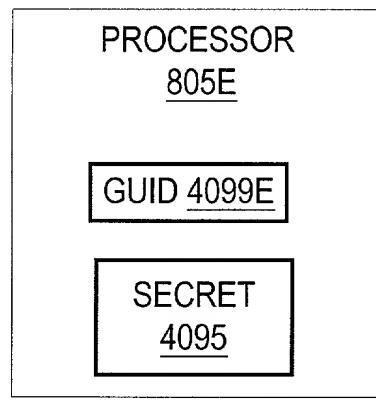


Fig. 29B

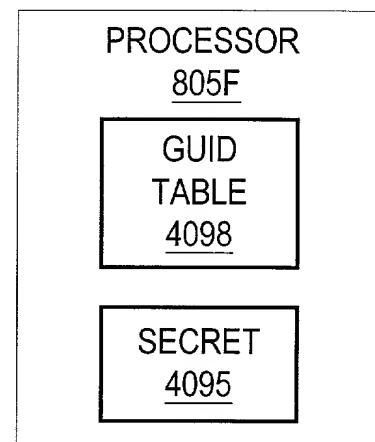


Fig. 29C

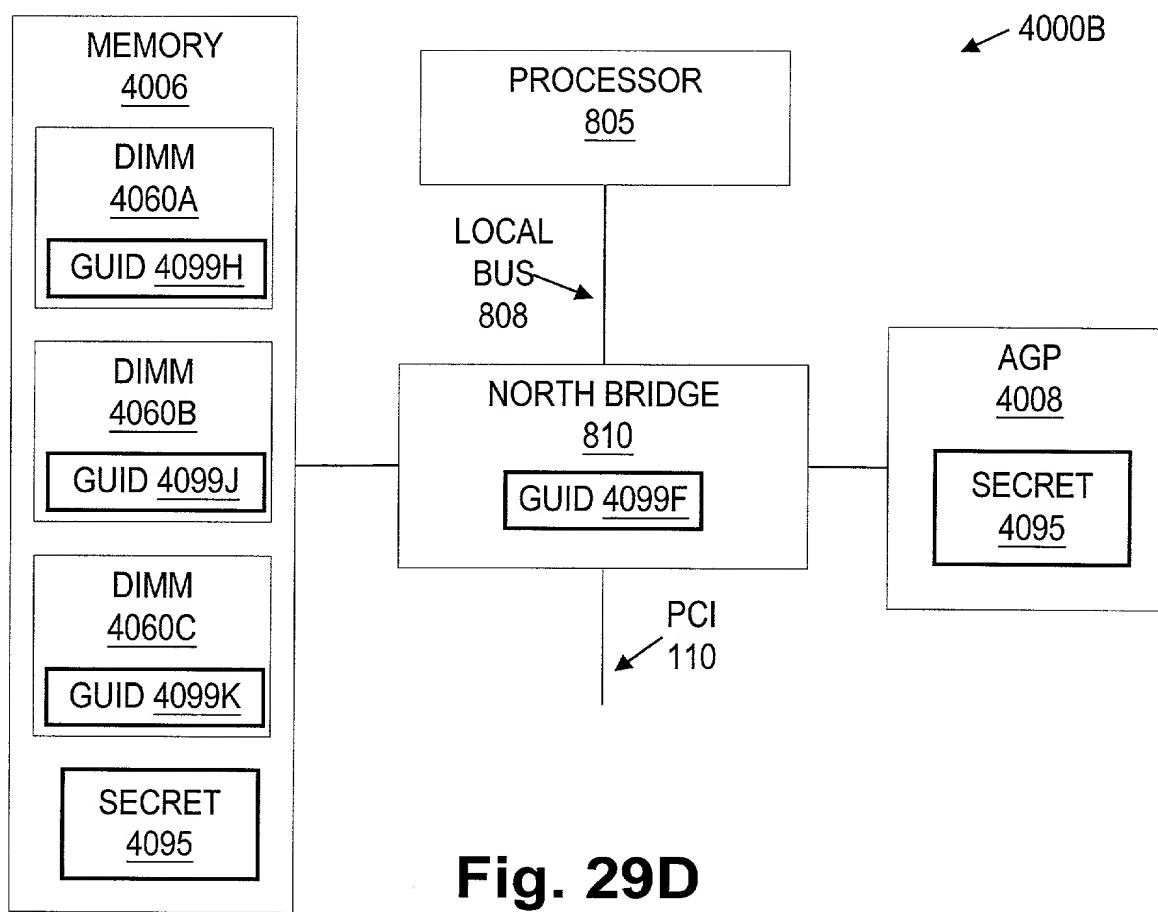
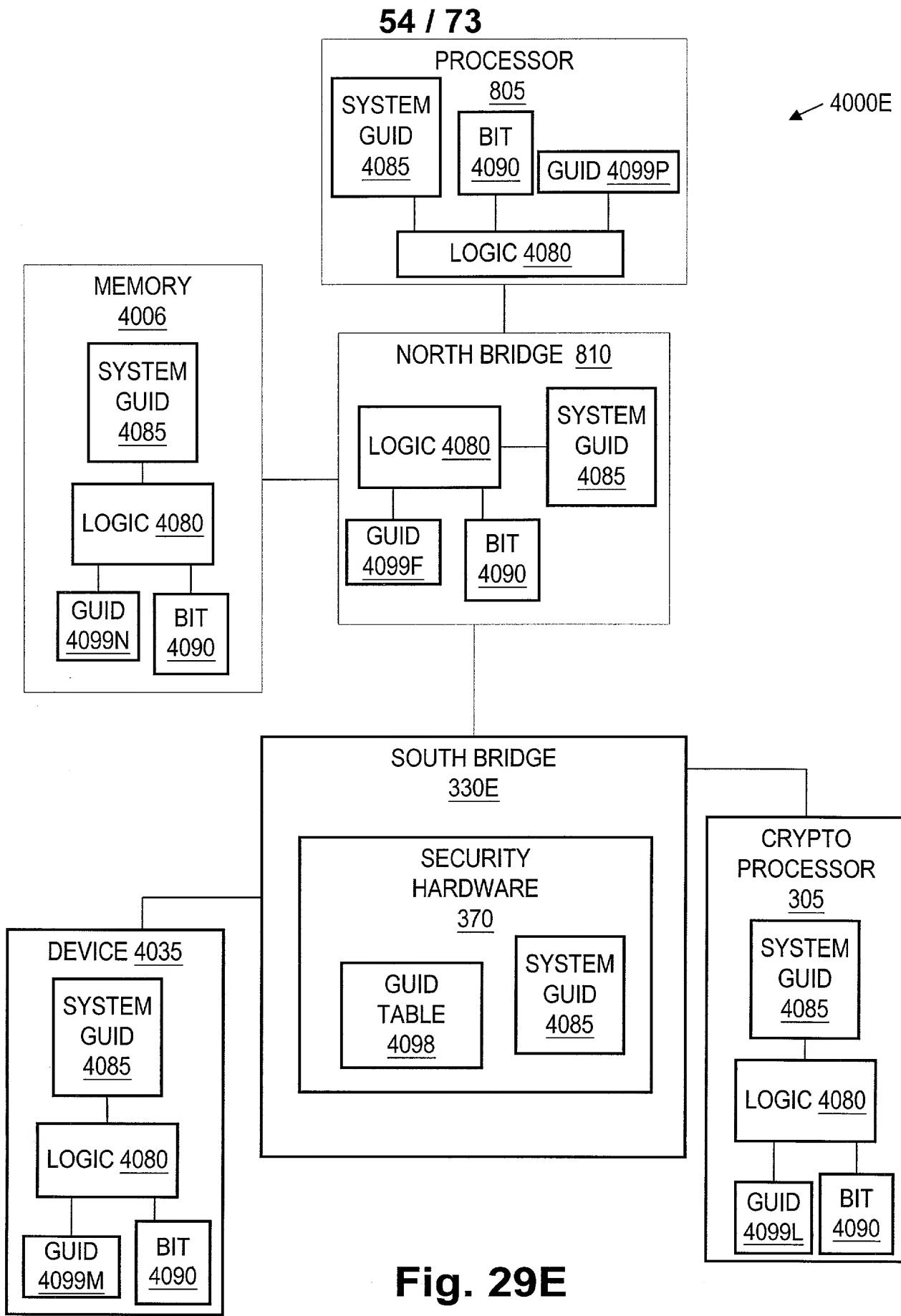


Fig. 29D

**Fig. 29E**

4100A

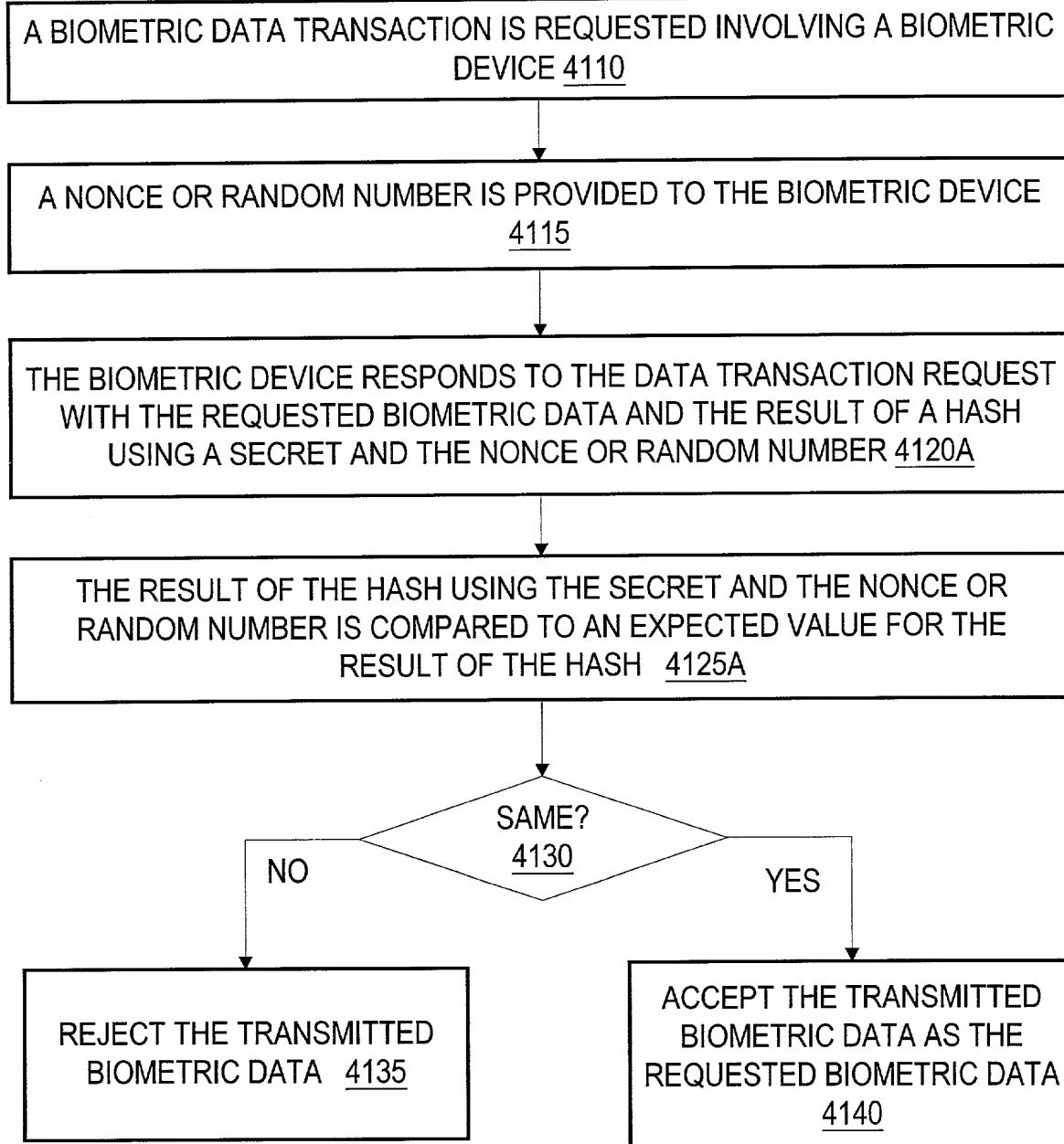


Fig. 30A

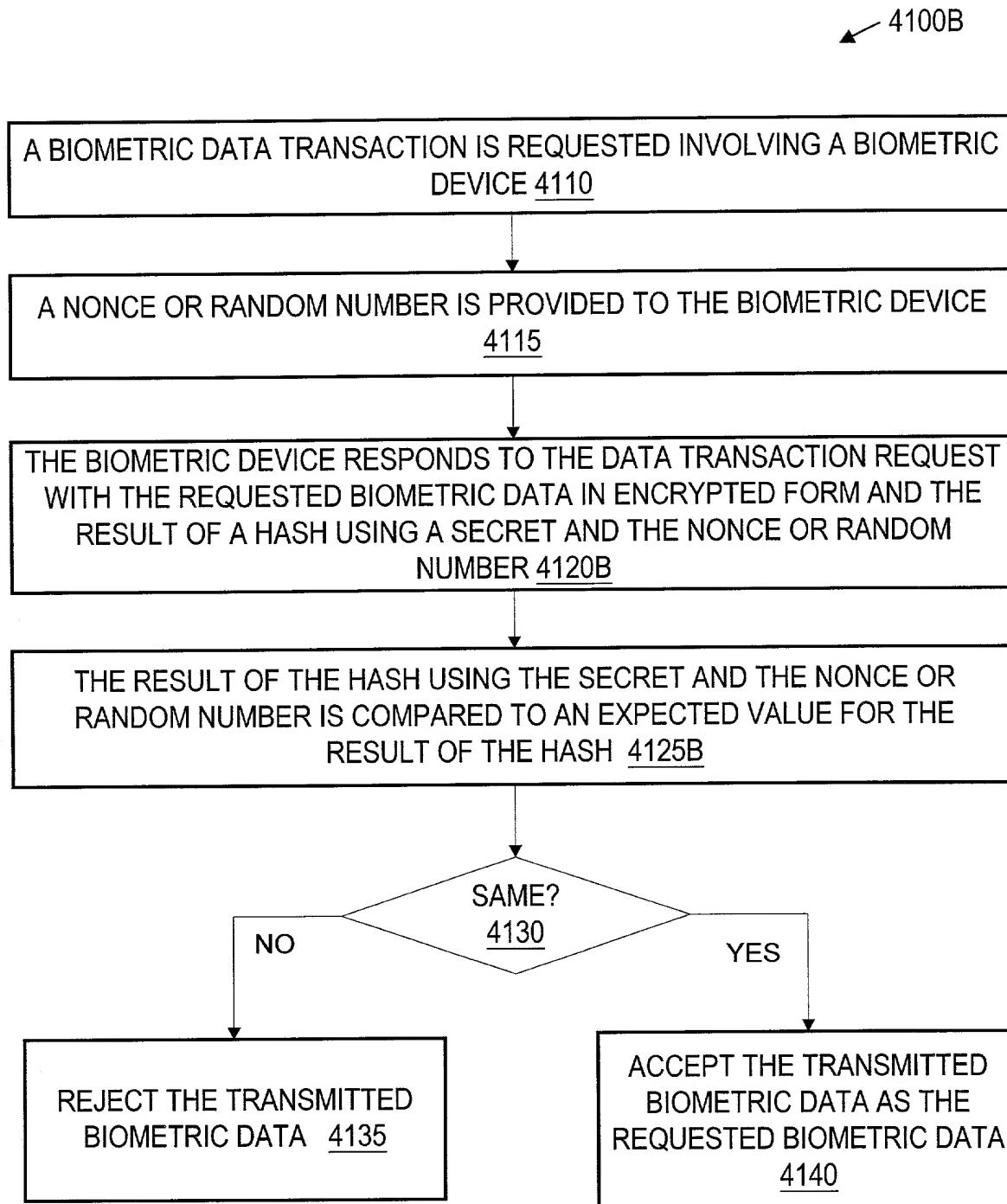


Fig. 30B

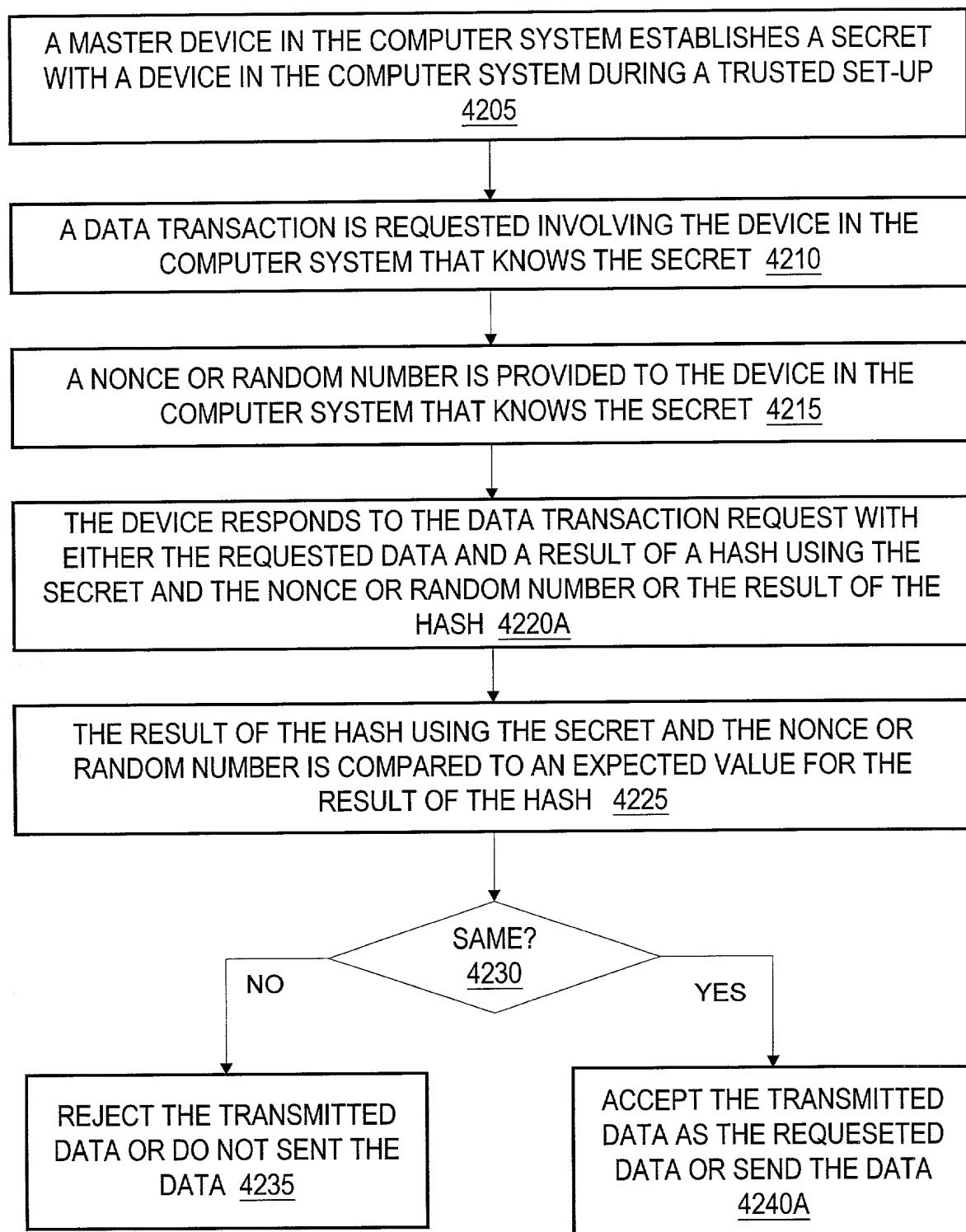


Fig. 31A

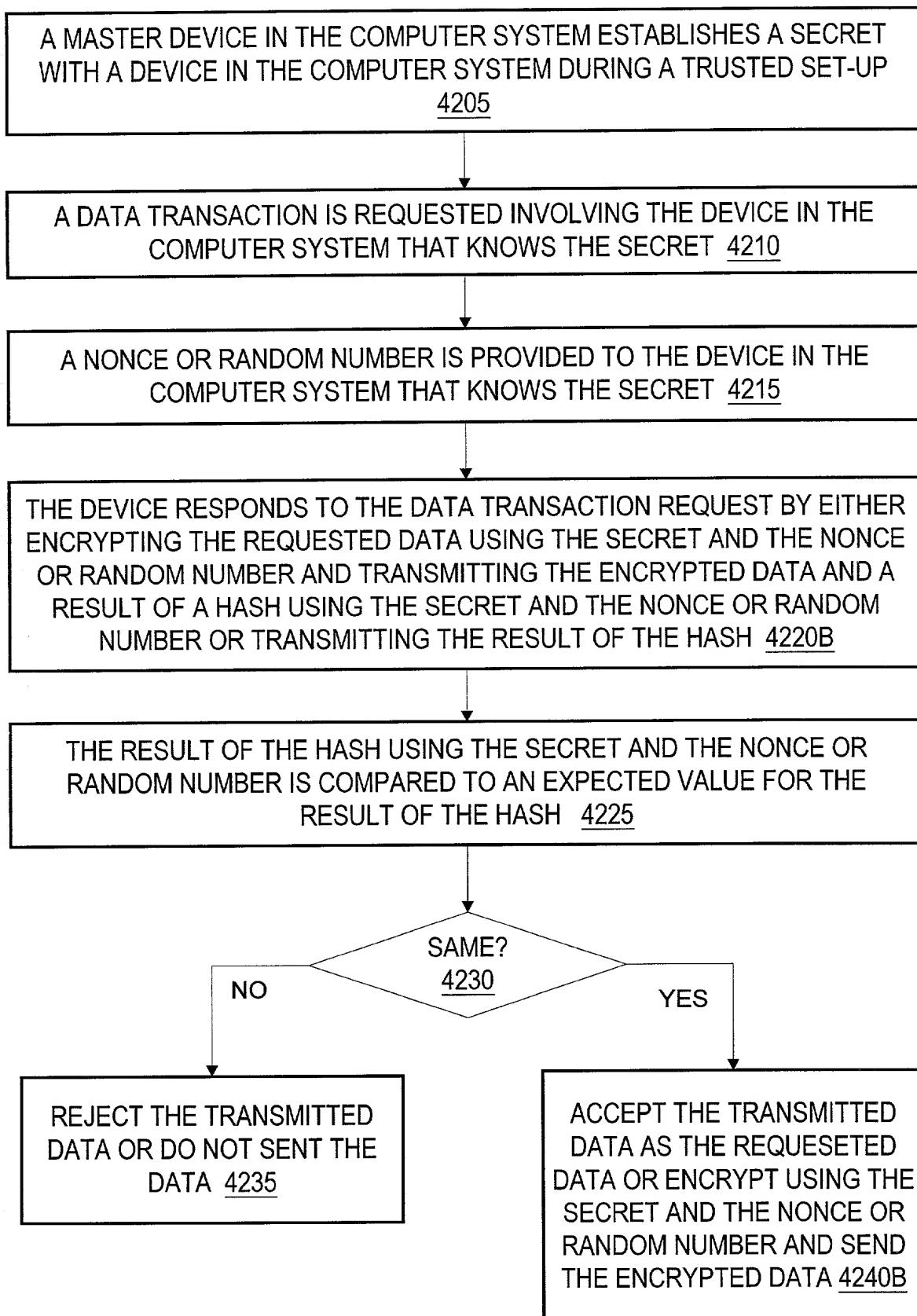


Fig. 31B

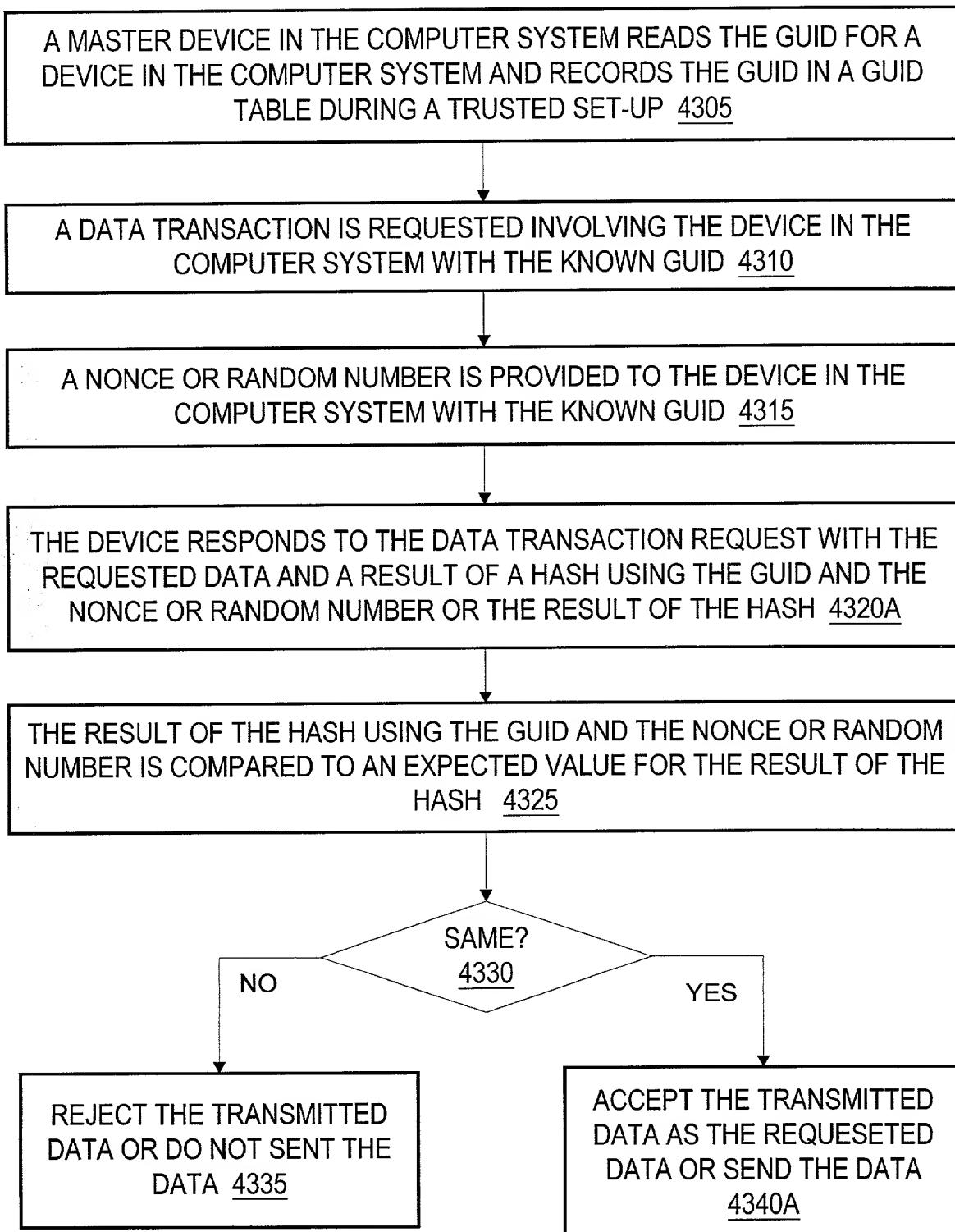


Fig. 32A

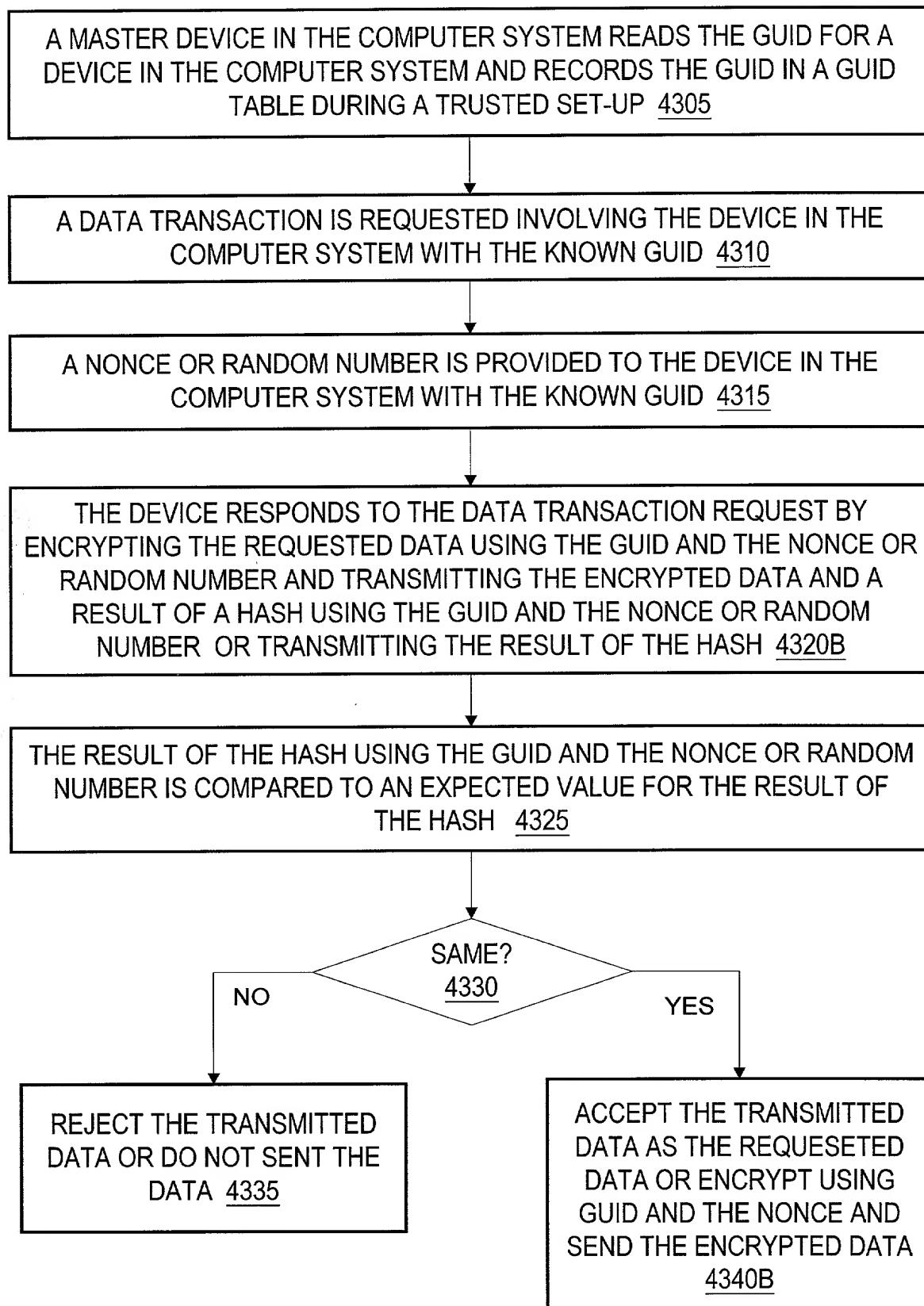


Fig. 32B

A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM, RECORDS THE GUID IN A GUID TABLE, AND TRANSMITS A SECRET TO THE DEVICE DURING A TRUSTED SET-UP

4306

A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET

4311

A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET

4316

THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4320C

THE RESULT OF THE HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4326

SAME?

4330

REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4335

ACCEPT THE TRANSMITTED DATA AS THE REQUESTED DATA OR ENCRYPT USING THE SECRET, THE GUID, AND THE NONCE AND SEND THE ENCRYPTED DATA 4340C

Fig. 32C

4400

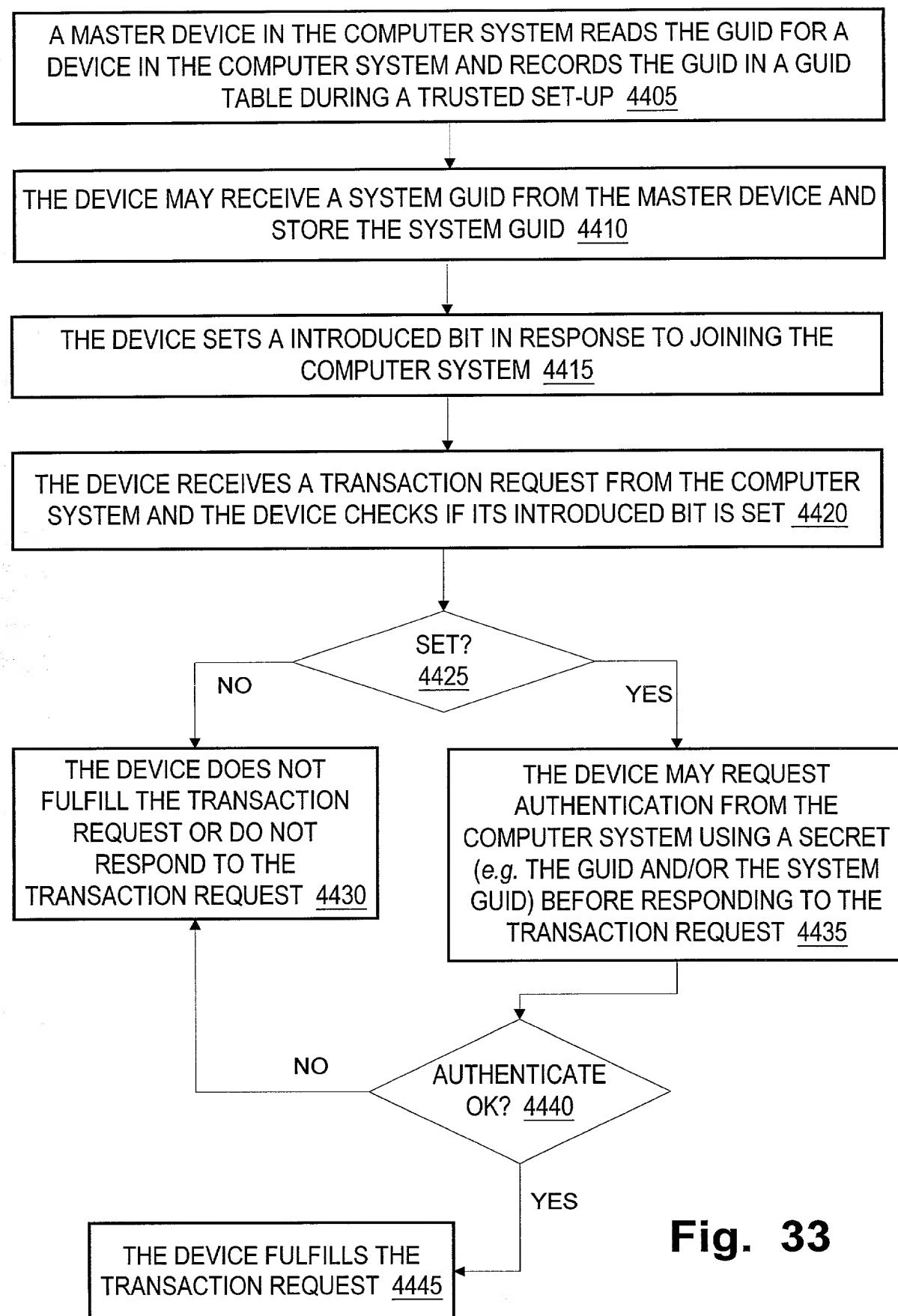


Fig. 33

63 / 73

4500

THE DEVICE OR THE MASTER DEVICE INITIATES A REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4505

THE DEVICE AND THE MASTER DEVICE AUTHENTICATE EACH OTHER USING THE GUID AND/OR THE SYSTEM GUID IN RESPONSE TO THE REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4510

THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE AND THE MASTER DEVICE SUCCESSFULLY AUTHENTICATING EACH OTHER 4515

Fig. 34

4600

THE DEVICE RECEIVING A COMMAND FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4605

THE DEVICE RECEIVING A MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES 4610

THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE RECEIVING THE MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES 4615

Fig. 35

64 / 73

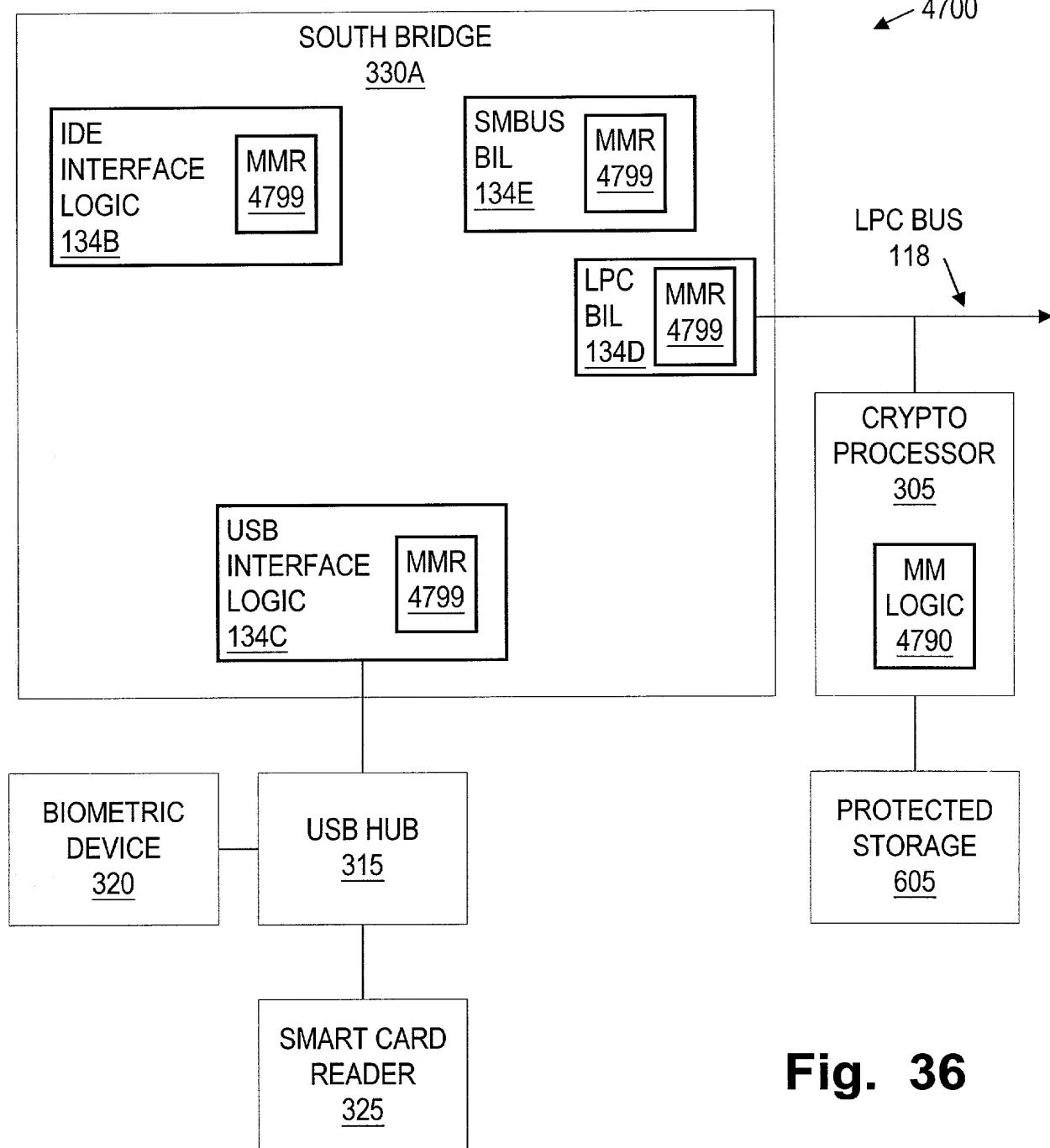


Fig. 36

TRANSMIT A MASTER MODE SIGNAL TO BUS INTERFACE LOGIC CONNECTED BETWEEN MASTER MODE LOGIC AND A DATA INPUT DEVICE, WHERE THE BUS INTERFACE LOGIC INCLUDES A MASTER MODE REGISTER 4805

4805

SET A MASTER MODE BIT IN THE MASTER MODE REGISTER(S) TO ESTABLISH SECURE TRANSMISSION CHANNEL BETWEEN THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM 4810

THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE EXCHANGE DATA OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM THROUGH THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4815

4815

THE MASTER MODE LOGIC FLUSHES THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER AFTER CONCLUDING THE DATA TRANSMISSIONS 4820

THE MASTER MODE LOGIC SIGNALS THE BUS INTERFACE LOGIC(S) TO UNSET THE Maser MODE BITS AFTER FLUSHING THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4825

4825

Fig. 37

09853226-05514C4

4900A

THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE
4920

ACCESSIONG THE SECURITY HARDWARE 4930

REQUEST AUTHENTICATION FROM THE CRYPTO-PROCESSOR USING
MASTER MODE 4935A

PLACE BUS INTERFACE LOGICS IN MASTER MODE 4938

RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE 4940

EXIT MASTER MODE AND FLUSH BUFFERS 4942

VERIFY AUTHENTICATION DATA 4944

VERIFIED?

4948

YES

NO

CONTINUE BOOT PROCESS 4990

Fig. 38A

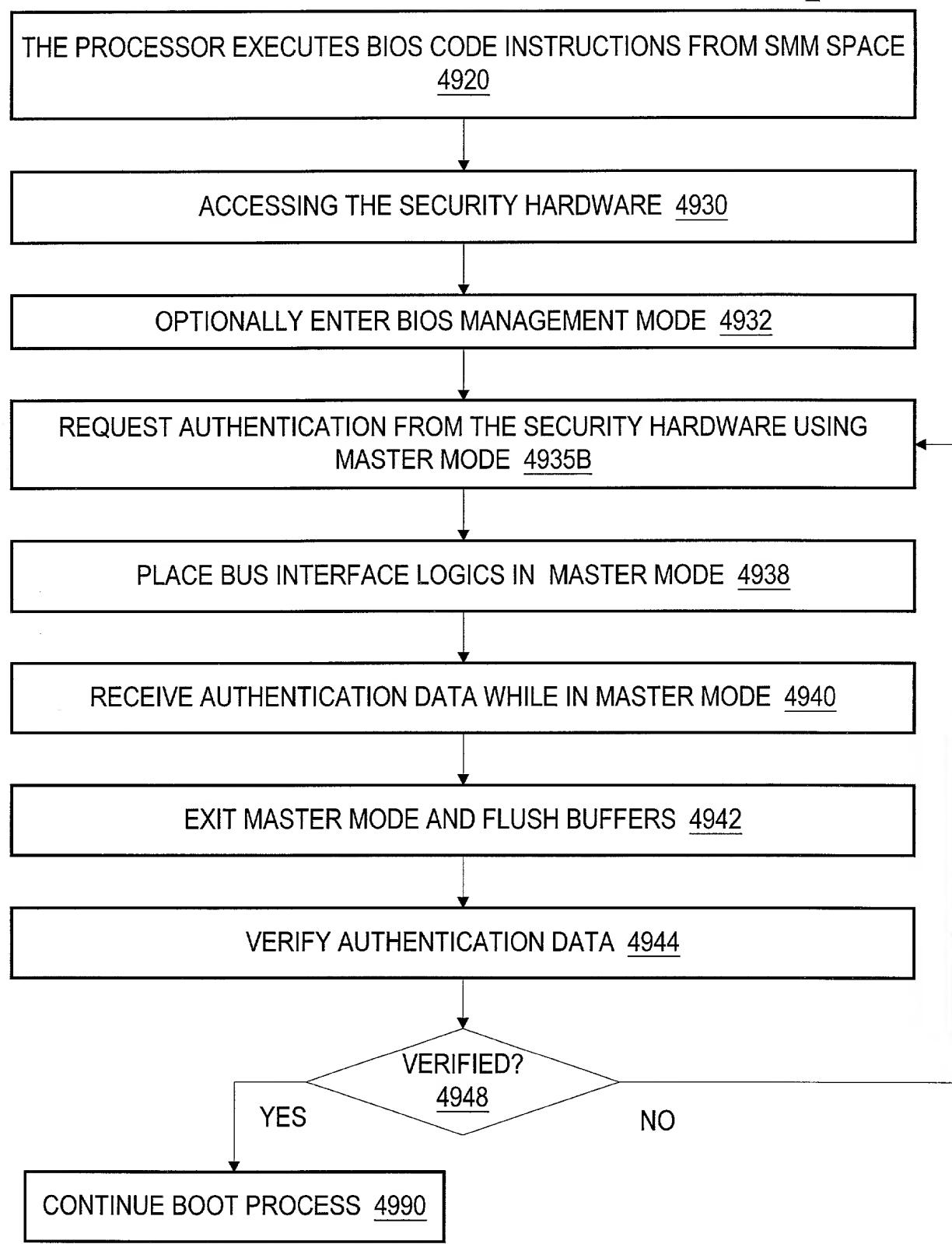


Fig. 38B

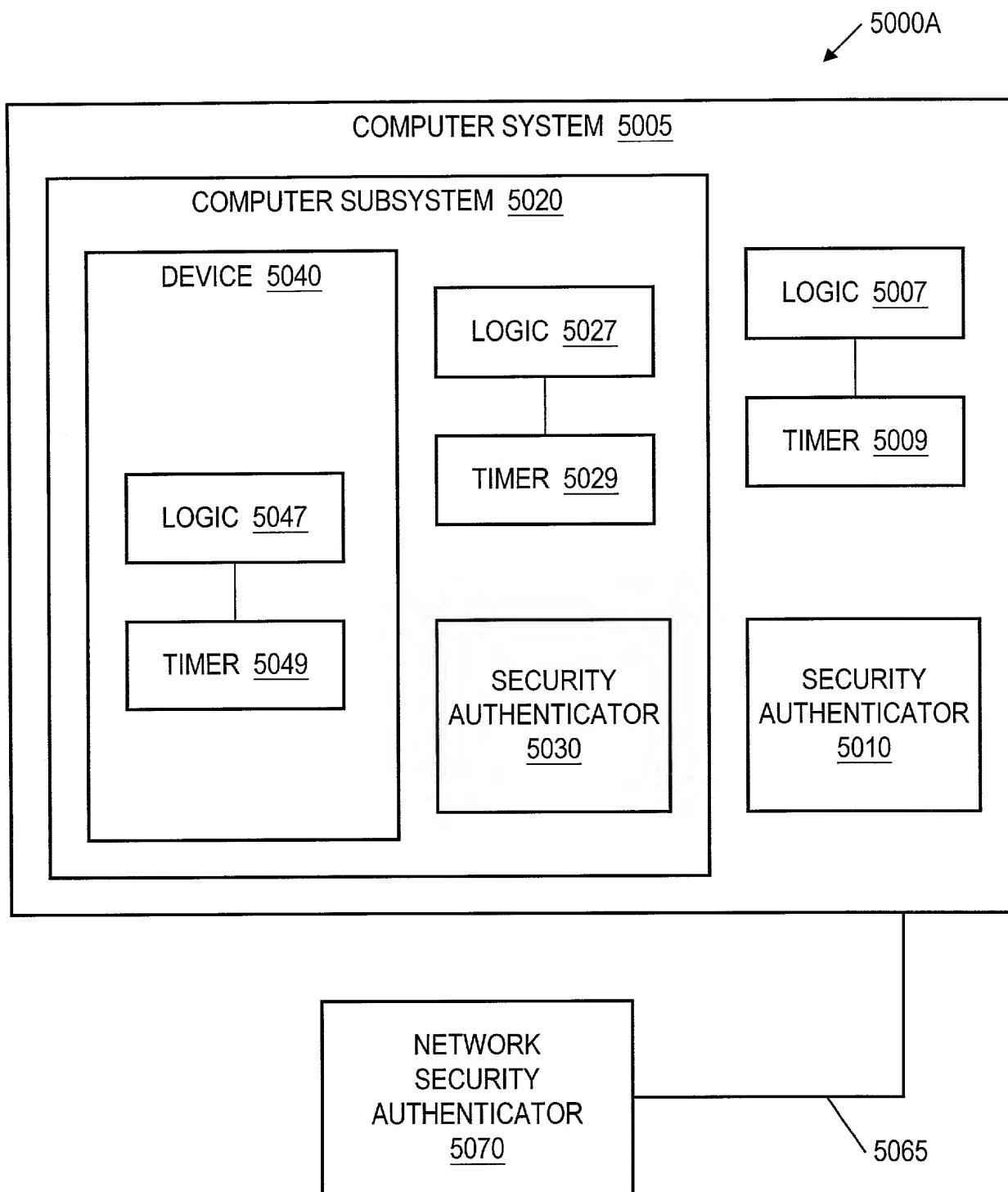


Fig. 39A

69 / 73

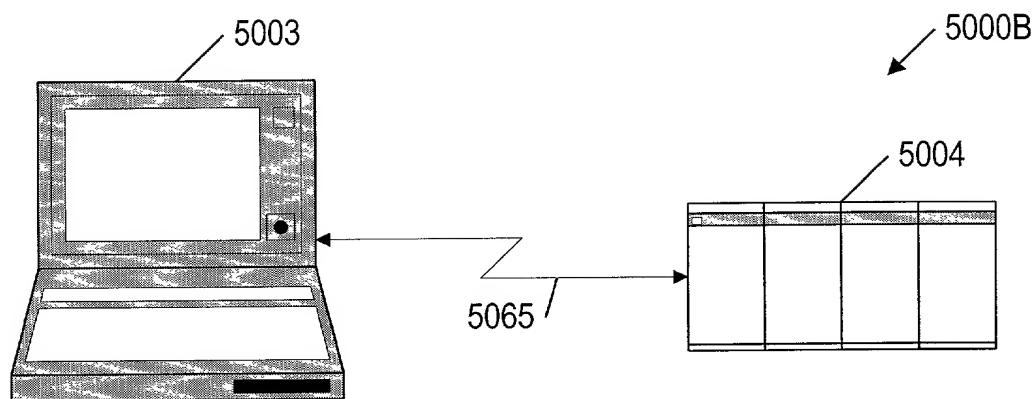


Fig. 39B

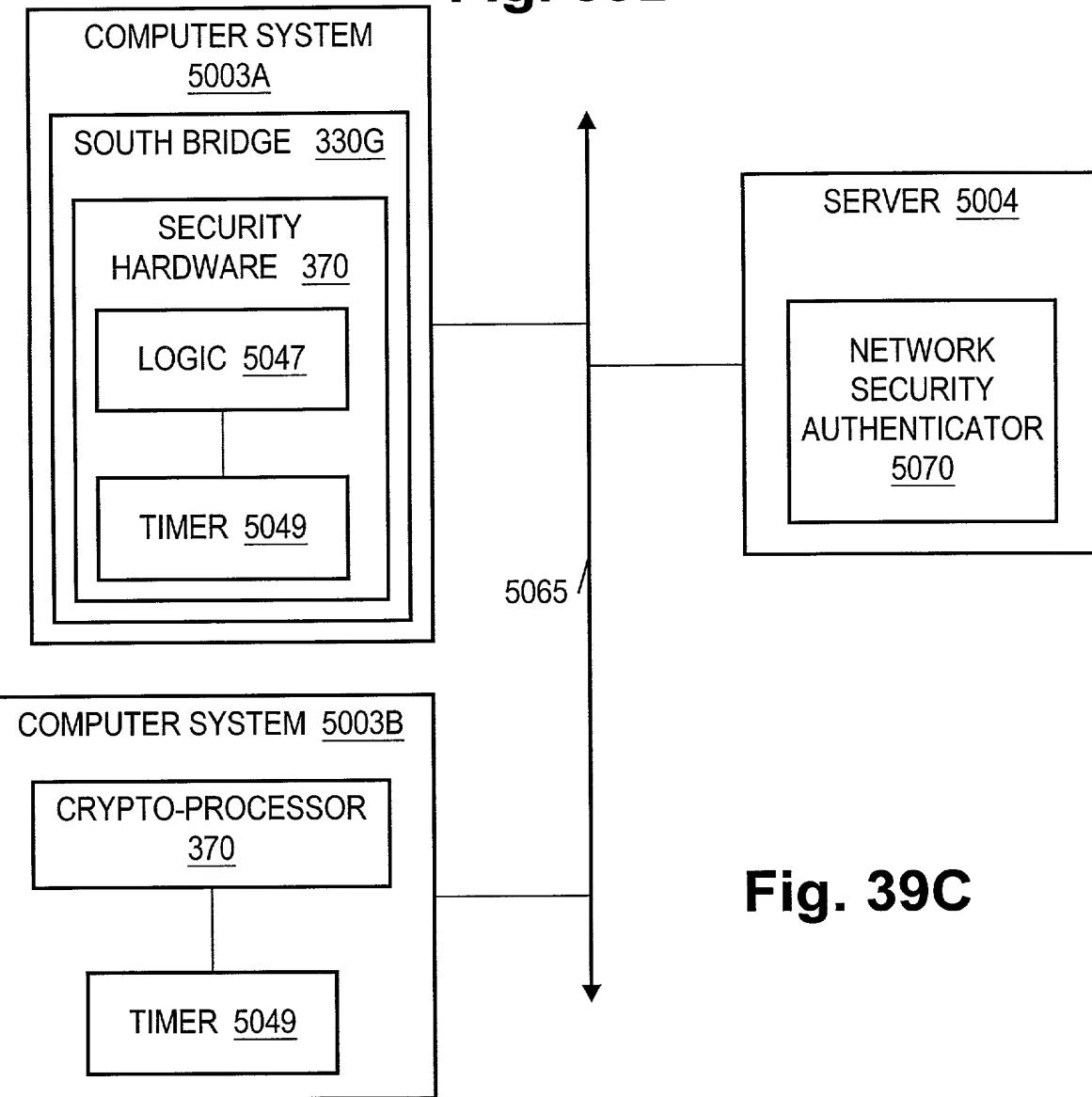


Fig. 39C

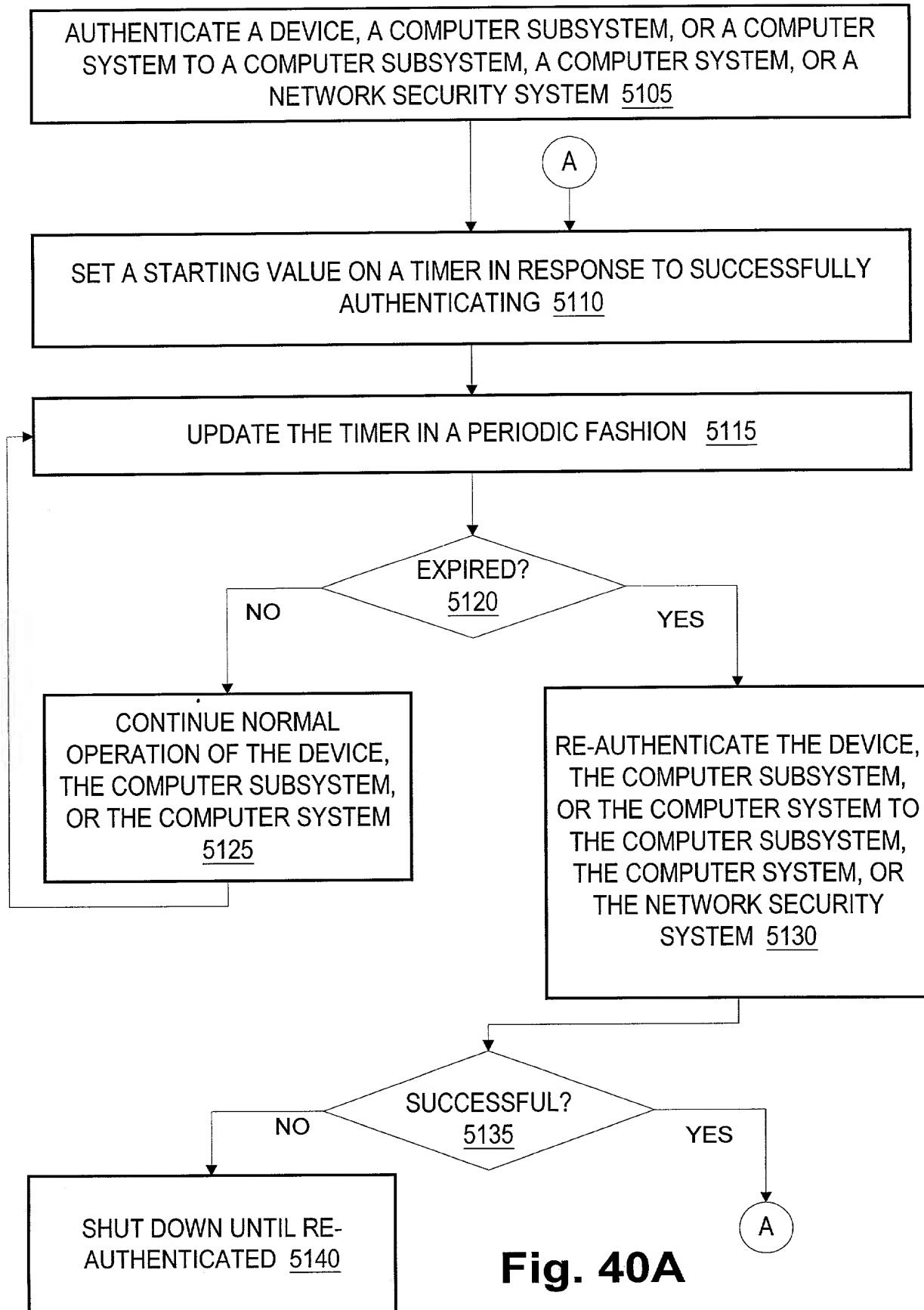
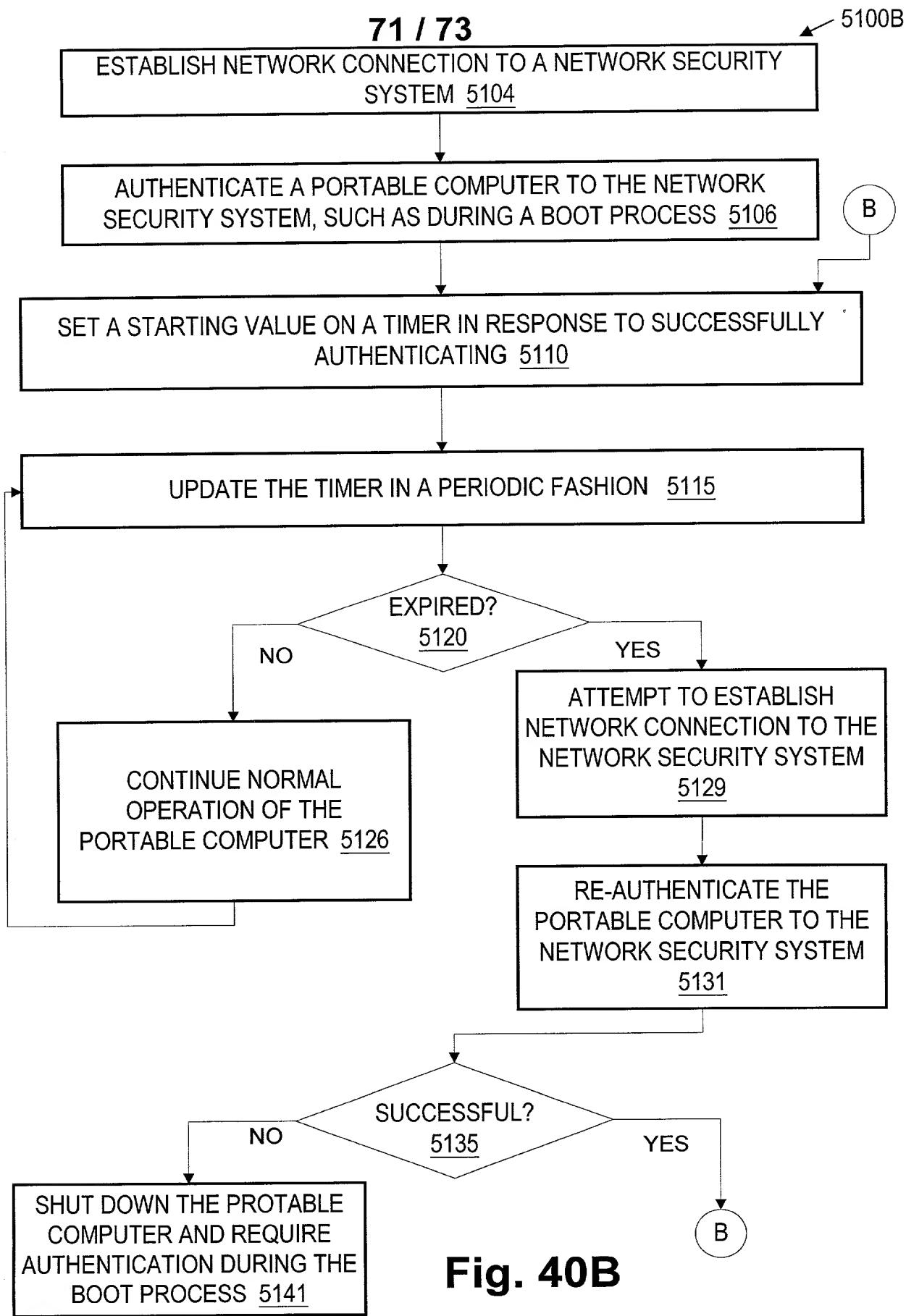


Fig. 40A

**Fig. 40B**

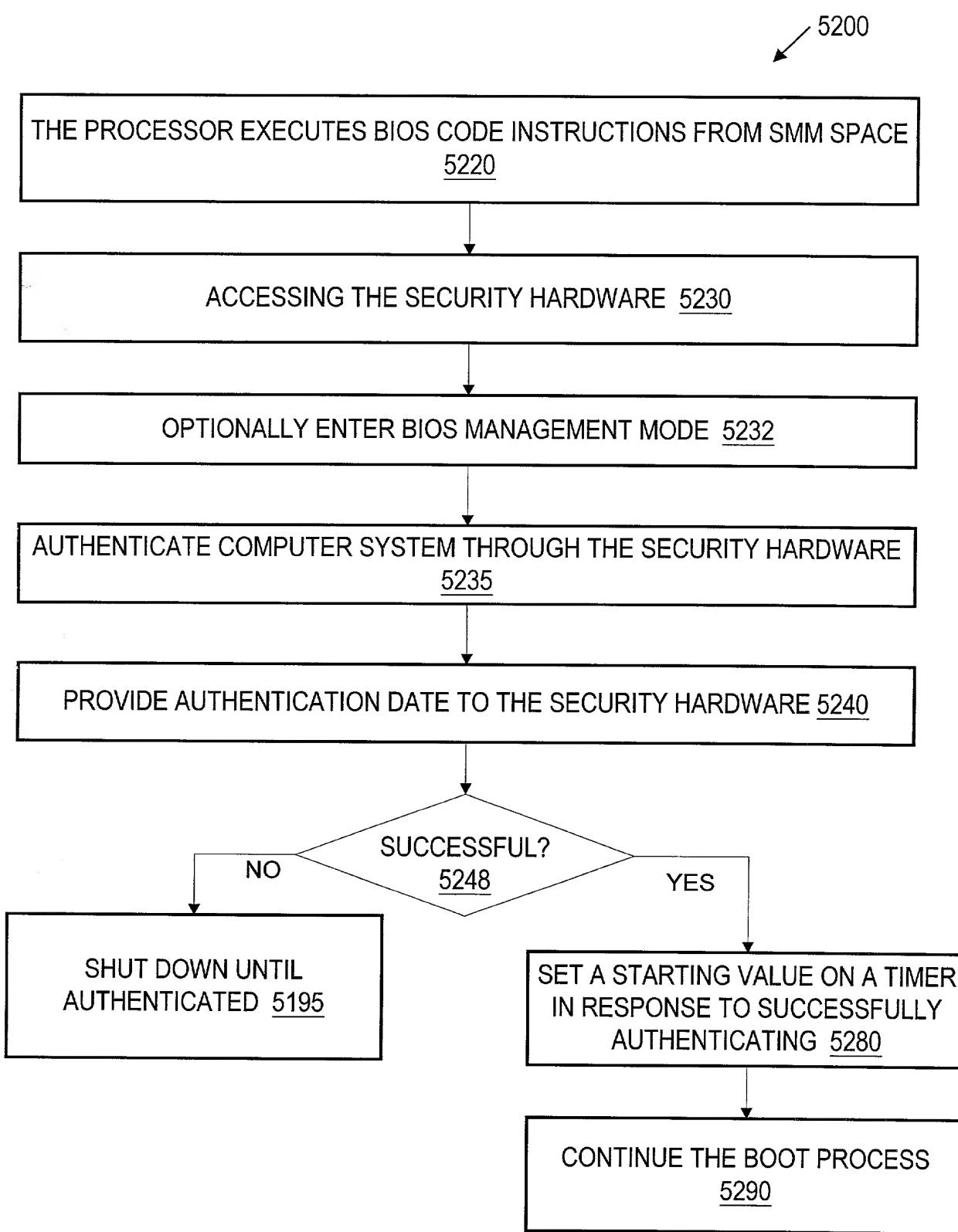


Fig. 41

73 / 73

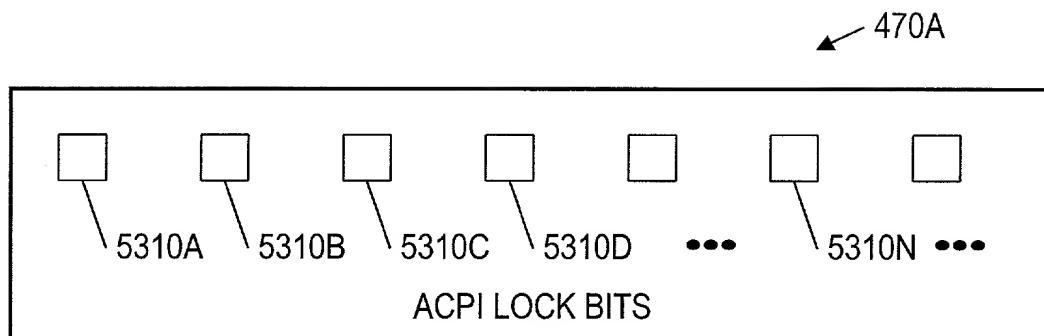


Fig. 42A

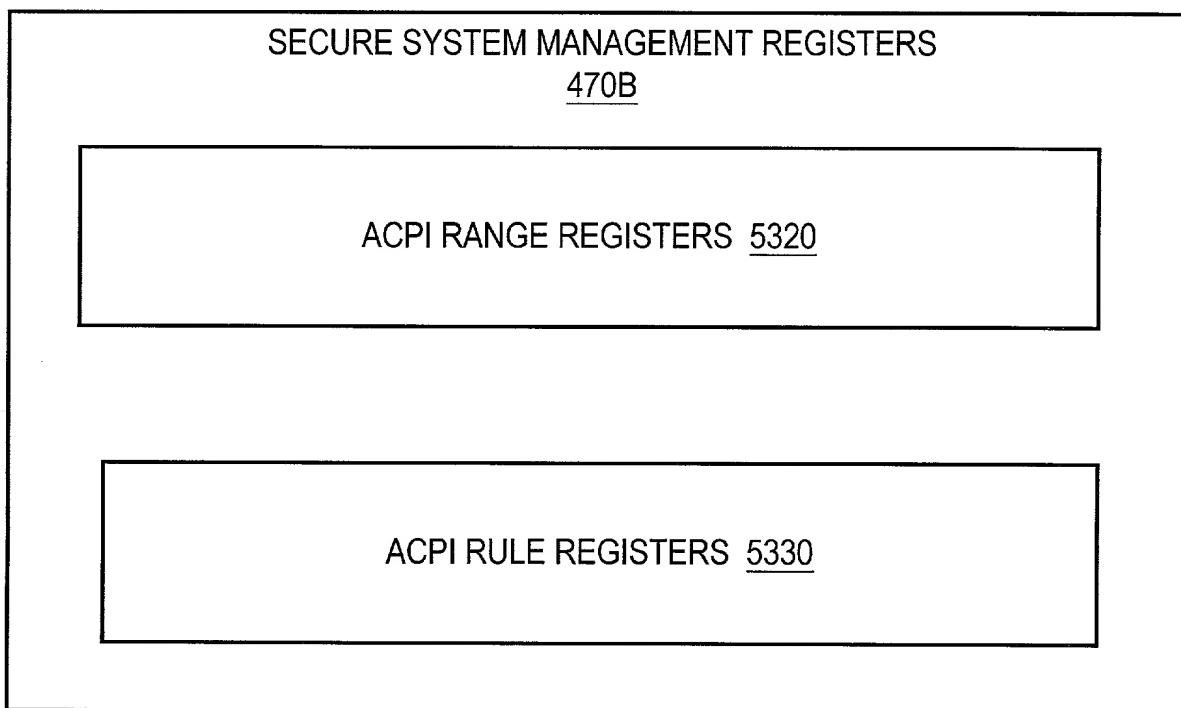


Fig. 42B